The design of future pre-payment systems

Ross Anderson | Johann Bezuidenhout | Neville Pattinson | Don Taylor

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

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

Schlumberger Electricity, Langer Road, Felixstowe, England IP11 8ER, neville@felixstowe.em.slb.com

Abstract

Over the next few years, the UK government plans to split the functions of electricity distribution and marketing. We discuss how prepayment and other metering systems can be adapted to cope. We propose a key management scheme whereby the distributor can delegate authority over a meter to a marketing company, which in turn can delegate to its agent. Our scheme controls risk by enabling the distributor to reconcile energy with cash and to revoke agents or even marketing companies that default, and to regain control over the meter.

1 Introduction

At present, the regional electricity companies are responsible for both the distribution and marketing of electricity. However, by April 1998 this will change: there will still be a single distributor in each geographical area, who will buy electricity from generators via the national grid and provide the reticulation with which it is delivered to homes and businesses. However, the end users will no longer have a contract with the distributor, but with a third party marketing company known as a supplier.

The suppliers will include the marketing arms of the existing distribution companies, but new marketing companies will be able to join the industry. They will purchase power from the distributor in half hourly slots, and sell the energy to users at whatever tariffs they care to devise[1]. They will not be restricted to a fixed geographical area, but will be able to supply nationally by having contracts with all distributors; it is expected that these new suppliers will include organisations such as banks and supermarket chains.

[1] subject of course to regulatory approval

Customers may have a contract with only one supplier at any time, but will be able to change their suppliers if they wish, subject to whatever contract terms the suppliers impose[1]. They will also be able to buy electricity from the supplier through agents, which might be conventional shops, telemarketing firms or even sites on the worldwide web.

There are a number of interesting aspects to this exercise, and the one which we propose to tackle in this paper is metering. How can this be supported in a secure and economic way?

2 The future challenge

To state the problem succinctly, we have only a few years to design and field systems which will allow multiple marketing entities to supply utility services through common vending and supply networks to geographically dispersed customers. Introducing arbitrary intermediaries means that distribution systems must provide remote control over the delivery of the utility service to the customer.

We do not assume that electricity will be the only utility affected. Water and gas may follow, as could the provision of communications services as electricity companies move into the telecomms business. Conversely, existing telecomms companies might become suppliers of electricity to help them sell packages of services. There may be horizontally integrated companies that provide telephone, cable TV, gas, electricity, water, burglar alarm and fire alarm services to a household, and manage the relationship by means of a single integrated communications system.

However, we expect that there will be other business models as well, including the current more vertically integrated one. There will almost certainly be applications that need an offline system, and not all customers will be creditworthy. This leads us to conclude that pre-payment meters will be an important part of the solution.

Of course, many customers in the UK demand credit meters, and see prepayment as a mark of low social status; but a pre-payment meter mechanism can be overlaid with billing functions to give a more general credit control system. The fundamental issue is the secure transfer of information to and from the meter; if we can do this well — which we need to do anyway for prepayment customers — then we can overlay not only credit billing, but also new options such as online payment over the Internet.

For all these reasons, it is important to get the prepayment system mechanisms right. Experience of existing systems [AB95] is that this takes more time than one is likely to anticipate; if a start is not made soon there is a chance that the system will be late and that many of the marketing options will limited or lost to the UK electricity distribution industry.

3 Prepayment basics

Slot meters were used in Britain for many years for both gas and electricity. However, the collection costs were high; the meters were the target in 54% of theft from some local authority housing [Par86] and the collection staff were also vulnerable to attack [AG90]. This led to the development in the UK of meters that used electronic tokens, such as smartcards and EEPROM key devices.

In South Africa, it is a national priority to electrify another two million homes by the end of the century, and prepayment meters will be used for most of these connections. This has created the fastest growing prepayment market in the world, and given the diversity of suppliers we have learned a great deal about the real costs and benefits of various technical alternatives [AB96]. The tokens used have included disposable cardboard tickets with magnetic strips, and 20 digit numbers printed at the vend point on a slip of paper and entered by the customer at a keypad on the meter.

US manufacturers have experimented with packet radio, so the token might not even have a physical form at all. It is simply a channel for transferring information to (and in many cases also from) the meter.

The information that it transfers may be vulnerable to replay and other manipulation. This is easy with numeric tickets, slightly harder with magnetic tickets, and fairly difficult with smartcards; but it is always possible [BFL+93]. So a prudent manufacturer will assume that manipulation attacks will happen, and the transfer instruction information is now commonly encrypted. The use of cryptographic techniques in prepayment meters is discussed in [AB94]; a general textbook on cryptography is [Sch95].

The authors of this paper have between them very extensive experience of prepayment meter systems in both the UK and South Africa — the two countries with largest fielded systems — and we hope that this experience can be applied to the current challenge.

The South African system supports most of the features that next generation European systems will need, including a national multi supplier vending network which can support customers at the vend point of their choice, meters that can be moved from one supplier's key to another, sufficient security to ensure that value transfers are not tampered with; and a robust means of settling the money due to and from various suppliers. Some features need to be added, such as the ability to program meters with new tariff structures. Its main weakness is that the information flow is one way — from the supplier to the meter — and there is no provision for sending meter readings and power profiles back to the supplier. Balancing energy with cash thus involves tracking moving averages of sales against feeder meter readings.

The UK system tackled this weakness by introducing an electronic token in the shape of a key. This made it possible to transport information in both directions; each time the token is moved between the point-of-sale equipment and the meter, an EEPROM within the key carries credit and tariff data to the meter, and takes a complete meter reading and status information back to the company. With this two way link, a security system was devised to ensure that data tampering, replay, and other forms of attack were difficult and detectable. The more high-tech and high-cost approach was justified given the local technical infrastructure and economics.

But the UK system is now running into problems. When it was developed, the industry was fully nationalised, so one specification suited all needs; the security system only had to protect the utilities from third party attack rather than from each other. It was designed around a proprietary technique [VK84], and was so successful that a second manufacturer had to be licensed to cope with demand. However, the second supplier used a different proprietary security technology, so the point of sale infrastructure then had to be updated to cope with two different systems.

However, the original designs did not cater for fully competitive supply. It is becoming clear that the security specification must change significantly: it must not only protect commercial rivals from each other, but since the system moves both credits and tariffs around, the fraud risks are more complicated, and the security mechanisms must be correspondingly more flexible and robust.

4 System security requirements

In order to meet the challenge described above, we will need to develop a system, rather than just a meter protocol. Experience in both the UK and South Africa shows that the critical success factor is not so much the individual security mechanisms chosen, but the care which is taken to make them work together as a whole integrated system.

This system will involve transactions between a number of different parties. Their identities are not yet settled; we do not know, for example, whether it will be the distributor who is responsible for managing cryptographic keys and for keeping the payment mechanism generally sound, or whether this responsibility will pass to new bodies reporting to the Customer Supply Code Executive (CSCE). We will assume here that it will be the distributor; a separate CSCE body can be accommodated with minor changes.

The main processes that need to be secured are:

- the energy accounting systems of the distributors and the suppliers. The distributor buys metered energy from the grid and has to pay for it. He will need a system to detect non-technical revenue losses such as those caused by customers bypassing and tampering with their meters. This means interfacing closely with:

- the financial bookkeeping systems of the distributors, the suppliers, and the agents. Of course, as with all bookkeeping systems, these need to be designed carefully in order to control the kinds of fraud carried out by staff in any business. Particular care has to be taken to prevent collusion between wholesale staff and the agents who actually collect money from the public, which in turn needs a clear interface with:

- the vending system used by the agents to sell tokens to the public. These require the usual balancing controls found in other retail terminal equipment such as shop tills and lottery ticket terminals. However they also need to contain cryptographic key material in order to generate valid token information for transport to meters, and communications to relay information back from the meters to the distributor (this information might include a history of power consumption by time of day, and tamper occurrences). Thus:

- the meters need to be physically robust in order to make tampering difficult. They must also be certified which means that if new software is to be loaded whenever the customer changes supplier, then the meter must be able to check that this software has indeed been certified. So each meter needs to contain one or more cryptographic keys, which need to be managed in such a way that all the parties have a reasonable degree of protection against fraud by the others, and that they can all trust the system to protect their interests.

If these systems do not work well together, then it can be very expensive indeed for the distributors, the suppliers, the agents, the meter manufacturers — and ultimately the customers. Examples of security failure are given in [AB94]; some of them cost millions to put right. There is also the delay, confusion and reengineering which can result if, for example, one designs an agent vending system to operate online and then finds in the field that offline operation is needed.

The intangibles are also very important. The consumers must trust the meters; the distributors and suppliers must trust the vending system to inform them of all sales; and the all parties involved must trust the settlement system. The formal chains of accountability for settlements and for meter certification pass through OFFER to parliament; mechanisms for handling customer complaints must also be set up, and ought to be designed to avoid the bitter controversy that has dogged complaints about phantom withdrawals from automatic teller machines [And94]. In this respect, it is important that the complaints bureau should not be seen as an industry captive.

Finally there is an unseen but vital technical component — the key management — which we absolutely need to get right. In our experience, this is one of the most important, and most difficult, design problems; it is one in which the majority of published designs, and a significant number of international standards, have turned out to possess serious flaws [BAN89] [AN95]. However, it is a problem with which both UK and South African industries have now amassed a lot of (expensive) experience.

5 Proposal

The following proposal is based on the technology developed by Eskom for its meter system, and on the banking community over the last two decades to handle interbank automatic teller machine transactions. See [MM82] for a description of basic banking cryptography, and [And94] for its failure history. Further information on cryptography can be found in [Sch95], cited above, and [Sim92].

As discussed above, we assume that the distributor is responsible for installing the meters, and that the i-th meter is furnished with key KD_i. When the customer makes a contract with a supplier, the supplier will notify the distributor, who will issue a delegation message:

$$T_{DS} = \{KS_i, P\}_{KD_i}, \{KS_i, P\}_{KDS} \tag{1}$$

We use the notation of [BAN89]: the first component of this message consists of a time period P (starting and expiry dates) and a supplier meter key KS_i, both encrypted under the key KD_i which the distributor shares with the meter; the second component contains the same information encrypted with a key K_{DS} which the distributor shares with the supplier.

The supplier can now issue $\{KS_i, P\}_{KD_i}$ to the meter in a token, which will clear any previous supplier meter key from the start date of P. The supplier may then issue instructions to the meter using KS_i until the expiry date of P. The supplier may also wish to load his own software into the meter (as otherwise tariff complexity would be a limiting factor to competition), and this software may be certified using an authentication code calculated by the distributor using KD_i.

The customer may now wish to buy tokens from an agent. For example, he might commute to London from Norfolk, and wish to buy tokens for a Norfolk meter from a shop in the City. This means that the London agent must either be online all the time, which is expensive, or share a key with the customer's meter.

However, we do not want every agent to have a key for every meter, since then the return from subverting an agent's equipment would be the ability to sell tokens to anyone in the country. Although tamper-resistant devices such as smartcards can give some protection to crypto keys, this protection is never complete (see [BFL+93] for the reverse engineering of silicon chips). In any case, the storage required for some 20 million keys would be of the order of 500 Megabytes which would be expensive.

Our solution is to use intelligent cacheing. The customer is issued with a card with his ID and a crypto checksum. The checksum is like a banking CVV — a three digit value on card magnetic stripes that prevents dishonest retailers from manufacturing a card or otherwise impersonating the customer unless they have actually had her card in their possession.

When the customer presents his card to a vend point, the agent goes online to the supplier. Provided that the account is in good standing and the checksum is correct, the agent gets the customer's current meter key KS_i, encrypted under a key K_{AS} shared between the agent and the supplier, together with a new checksum which is written to the card.

The agent always keeps the keys KS_i in tamper-resistant storage. As noted above, we assume that penetrations will still be possible at a certain cost; so we limit the gains from a successful penetration by letting the agent store only a few thousand keys at any one time. This way the customer can buy tokens online anywhere, and can also buy from his usual agent while the system is offline — giving an acceptable tradeoff between performance and risk.

Controls should be end-to-end where possible, and in the present case it is important that the distributor (who owns the meter and pays the grid for the electricity) should exercise the primary control over fraud. In the South African system, which has no return channel from the meter, energy delivered through feeder meters is balanced against a moving average of sales.

This simplification has led to equipment cost savings but has added to the complexity of system operation; the UK solution of using the payment token to provide a return channel is better in environments where the token technology and telecommunications infrastructure are available, and where labour is more expensive. In this case, the goal of end-to-end control can be achieved by encrypting the return information under a key shared between the meter and the distributor.

Another advantage of our proposed solution is that the transactions needed to support delegation from distributor to supplier, and from supplier to agent, are sufficiently like those already used to manage keys in banking networks that they can be implemented easily on standard banking encryption products (Eskom uses IBM TSS equipment [JDK+] but there are plenty of alternatives).

6 Conclusions

Britain's new electricity marketing regime will bring the industry many challenges. We will need to construct a robust and secure national network that lets customers move their custom to the supplier of their choice and buy tokens from the agent of their choice.

We believe that experience in both the UK and South Africa can save the industry from reinventing the wheel. We have sketched mechanisms to delegate control over meters from distributors to suppliers and from there to agents. Our philosophy is to locate the complexity where it can be accessed and managed (in the distributors' and suppliers' systems) while simplifying the most numerous items (the meters). We also provide end-to-end control of customer key material so that suppliers who misbehave may be detected and revoked without having to physically replace meters.

We hope that our proposals may serve as a basis for discussion, and get the IEC TC13 WG15 standardisation effort off the ground.

References

[And94] RJ Anderson, "Why Cryptosystems Fail", in *Communications of the ACM* v 37 no 11 (Nov 1994) pp 32–40

[AB95] RJ Anderson, SJ Bezuidenhout, "Cryptographic Credit Control in Pre-payment Metering Systems", in *1995 IEEE Symposium on Security and Privacy*, pp 15–23

[AB96] RJ Anderson, SJ Bezuidenhout, "On the Reliability of Electronic Payment Systems" to appear in *IEEE Transactions on Software Engineering*

[AG90] 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

[AN95] RJ Anderson, RM Needham, "Programming Satan's Computer", in *'Computer Science Today — Recent Trends and Developments'*, J van Leeuven (ed.), Springer Lecture Notes in Computer Science volume 1000 pp 426–440

[BAN89] 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

[BFL+93] S Blythe, B Fraboni, S Lall, H Ahmed, U de Riu, "Layout Reconstruction of Complex Silicon Chips", in *IEEE J. of Solid-State Circuits* v 28 no 2 (Feb 93) pp 138–145

[JDK+] DB Johnson, GM Dolan, MJ Kelly, AV Le, SM Matyas, "Common Cryptographic Architecture Application Programming Interface", in *IBM Systems Journal* **30** no 2 (1991) pp 130 - 150

[MM82] CH Meyer, SM Matyas, *'Cryptography: A New Dimension in Computer Data Security'*, John Wiley and Sons (New York, 1982)

[Par86] MJA Partridge, "Prepayment Coin Meters — A Target for Burglary", *UK Home Office Crime Prevention Report no. 6* (1986)

[Sch95] B Schneier, *'Applied Cryptography: Protocols, Algorithms, and Source Code in C'*, Wiley and Sons (2nd ed., New York 1995)

[Sim92] GJ Simmons, *'Contemporary Cryptology: The Science of Information Integrity'*, IEEE Press, 1992

[VK84] J Vaughan, K Lucking, "Electronic Key Prepayment Meter", UK Patent 2153573, filed 25/1/84, granted: 1/4/87

Ross Anderson received his MA and PhD degrees from Cambridge University, where he is a lecturer at the Computer Laboratory. He is a chartered engineer, a chartered mathematician, and a Member of the IEE. He has worked in computer security and cryptography for about ten years; his research interests include next generation payment systems, security protocols, cryptographic algorithms, information hiding techniques and statistical models of system reliability.

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 is a Senior Member of the SAIEE and a member of the Computer Society of South Africa. He has been employed by Eskom since 1980 where he has worked in nuclear reactor safety and computer security; he designed and established the systems with which prepayment meters are managed. His research interests include cryptographic key management and time coherence of information in distributed secure databases.

Neville Pattinson is Director of Product Development for Schlumberger Electricity in the UK and has been involved for many years in the development of electricity and water prepayment Key token operated meters and associated vending infrastructures. He graduated from Leicester Polytechnic in 1984 with a BSc in Electronic Engineering and is presently an Associate Member of the IEE.

Don Taylor is Technical Director of the Schlumberger/AEG Joint Venture in South Africa where he developed the first prepayment meter used in the electrification programme in 1986. He graduated from Cape Technicon in 1975 with an HNDT in Electrical Engineering, and is a Member of SAIMC.