

**Simon Rix**

A Curriculum Vitae

08 October, 2008

# Contents

<b>Introduction.....</b>	<b>3</b>
<b>CypheRix .....</b>	<b>4</b>
Overview.....	4
The Certified Audio Recording System .....	4
Evidence Enrolment System .....	5
Hardware Encryptors and Cryptographic Logic Cores .....	5
Side Channel Attacks .....	6
BetaResearch .....	6
<b>Irdeto / M-Net.....</b>	<b>7</b>
Phase 1 - Strategic.....	7
Phase 2 - Design and Specification .....	8
<b>Life Skills.....</b>	<b>9</b>
Cryptographic: .....	9
Hardware design: .....	10
Software and Embedded Microprocessor Design: .....	11
Broadcasting: .....	11
<b>Patents.....</b>	<b>12</b>
Patents Filed and Granted .....	12
<b>12 Years in M-Net / Irdeto .....</b>	<b>14</b>
The Early Years.....	14
The Analogue Era.....	14
The Digital Era.....	16
<b>Reason for Leaving M-Net / Irdeto .....</b>	<b>18</b>
<b>Earlier Employment.....</b>	<b>19</b>
1979 - 1983 SABC.....	19
1983 - 1984 SA Philips .....	19
1984 - 1986 Technikon Witwaterrand.....	19
<b>Personal Details.....</b>	<b>20</b>

## CHAPTER 1

# INTRODUCTION

My working life is divided into three phases, pre-M-Net, M-Net / Irdeto and CypheRix. The second two phases are Pay TV centric.

When I was retrenched from M-Net / Irdeto I began my own companies. I own two companies, CypheRix in South Africa and CypherManx in the UK.

M-Net / Irdeto was probably the most prolific hands on design phase of my career as I was a dedicated designer and design manager for more than 12 years. I was also very active in system design and I designed the original CA Architectures. I have eight world patents in the Pay TV arena mainly from the early digital era (circa 1992).

During my time at M-Net / Irdeto I implemented a multitude of custom integrated circuit designs. There were at least thirty different IC designs (although it must be noted that many were related).

I have more than 10 million Integrated Circuits of my design in the Pay TV market place from companies as diverse as Texas Instruments, Samsung, NEC and Fujitsu.

M-Net / Irdeto provided the experience and knowledge to allow me to start my own company.

I will discuss each phase of my career separately.

## CHAPTER 2

# CYPHERRIX

### Overview

When I realized that retrenchment from Irdeto was inevitable in Q4 1997 I investigated several job opportunities as well as starting my own company.

I was fortunate in having good connections within the Pay TV industry and I was able to obtain a contract to develop a new Conditional Access system for BetaResearch, a major Pay TV operator in Germany.

I did the complete Conditional Access System architecture for this project. Clearly my knowledge of the Irdeto CAM and Smart Card helped. The system design had novel symmetric key based hierarchies, which resulted in rich anti-piracy features (both detection and ejection). We also developed rigorous automated testing methods, which improved the quality of the resultant design.

As I was able to obtain this contract I began CypheRix and CypherManx. As I personally preferred to work in a contract manner, I decided to employ only contract staff. I was able to offer most of the design team that took the retrenchment option at Irdeto a position on the project. I was most fortunate as most of the senior designers did not want to re-locate to the Netherlands so I was able to quickly build up an experienced design team that could work well together.

The BetaResearch project was a large one and amounted to more than 25 man-years of work. Up to 16 development engineers were employed on this project at one time.

Subsequent to the BetaResearch project I chose to try and diversify away from pure Pay TV Conditional Access design. I elected to develop three product areas where two of areas had application outside of Pay T.V.

### The Certified Audio Recording System

The first product development undertaken is a system to enroll audio recordings as evidence, where it is possible to prove to the court that this recording has not been altered in any manner.

To this end we have developed a digital audio recorder with an embedded Smart Card as well as a family of USB Control tokens. The Smart Card inside the Recorder cryptographically certified the audio recordings as

they happen. The USB Tokens ensure that the Recorders are tightly enrolled and controlled during all stages of their life cycles.

This is not the place for an advert on the Certified Audio Recording System. All I want to do is to say what we have done and illustrate our design principles. Please look at my web site [www.cypherix.co.za](http://www.cypherix.co.za) for more details.

The cryptographic methods used are novel and make the Recorder intuitively secure. For example we create a new RSA key pair for each recording. The secret key (of the newly created key pair) is used to sign certificates of the audio recording. At the end of the recording the RSA secret key is deleted. The public key is certified by more senior keys and added to the recording so the certificates can be checked. Now without the secret key no one can change the certificates. As the secret key is deleted it cannot be discovered by any method such as poor application software, side channel attacks, intrusive physical analysis.

### **Evidence Enrolment System**

The audio only enrolment system was subsequently expanded to include the ability to sign electronic documents submitted to the recorder on the USB port. The documents are signed using the same 'one time' RSA key used to sign the audio stream. This effectively proved that the various elements were enrolled at the same time as the 'one time' RSA secret exponent is deleted at the end of the enrolment session.

### **Hardware Encryptors and Cryptographic Logic Cores**

We have developed a hardware-based encryptor for use on short messages. This device was aimed at Pay TV Conditional Access developers. The device was developed to conceptual form (a working prototype PCB) when we could demonstrate the concept. During an evaluation phase prospective market decided to enforce an internal (to that country) solution which closed the door to the main customer. There was not enough volume in the remaining customers to warrant completing the development.

The design was done in such a manner that I can later add the Smart Card chips from the Certified Audio Recorder or the USB token. This will allow remote cryptographic share scheme arming and RSA based key transfers.

The VHDL cryptographic cores (DES, SHA-1 etc) can also be used elsewhere for Certification products. For example I am able to build a Certified Hard Drive copier where I can make a source copy of a source hard drive and certify it at about 50 megabytes per second.

I have developed and sold PCI based products that were evolved from the original Encryptor. The main user at this time is the Be Deers group in South Africa.

## Side Channel Attacks

We have designed methods of extracting keys from Smart Cards by measuring the changes in power consumption that occur on the chip when the Smart Card processes a secret key.

We have been able to identify a 128-bit AES secret key from a 0.35 micron Smart Card.

We have developed and patented a mathematically provable method of defending against Differential Power Analysis.

This was developed to allow us to provide security solutions for Pay Television.

## BetaResearch

The design brief was to develop a new Conditional Access system for use in German Pay T.V. We developed the complete System Architecture, the Smart Card and Encryptor.

The System Architecture is the heart of the system. We designed a novel script like command set. This allowed the operator to build up complex messages that allowed him to control the viewing rights in ways that could be altered as the business situation changed. The basic of the command set was a number of simple primitive operations of two types downloading (keys, products and characterizations) and filters (simple filters which simply allowed the operator to filter on the presence of items downloaded. Hence if the user has say product 24 you could filter to see if product 24 was present and still valid and if it was to transfer the encrypted control word to allow the view to receive a T.V. program.

The key hierarchy was novel in that it allowed the system operator actively defend against piracy. In the event of piracy occurring the system also had features that allowed the operator to identify the root (mother) Smart Card that was used in the cloning and methods to eject them.

The Smart Card also had our DPA defense algorithms built in.

We developed an extensive suite of automated test suites for testing the Smart Card. This allowed the card to be re-tested on all functional aspects whenever the slightest change was made. In order to expedite testing we developed a 'C' model of the Smart Card's functionality which ran behind a DLL on a Windows 2000 PC. The same 'C' code was used to compile either the final Smart Card or the 'C' model. The test system could interface to either the 'C' model or the final Smart Card. This allowed us to speed up testing as tests ran much faster on the PC and were much simpler to debug (both the Smart Card code and the test scripts). For final testing we had 12 Smart Card readers testing Smart Cards in parallel. A complete set of tests ran around 24 hours.

## CHAPTER 3

**IRDETO / M-NET**

Prior to starting my own company I worked at M-Net, a South African Pay TV operator, which developed their own Conditional Access technology. The technology group later became known as Irdeto Conditional Access.

When I left in 1998 I held the position of Systems Architect (Conditional Access and Cyphers) in the systems group within Irdeto.

Irdeto is a company dedicated to providing Pay TV products within the MIH group as well as to external clients on a world-wide basis. It has provided complete pay TV solutions for M-Net in South Africa, Telepiu in Italy, Filmnet in Benelux and Scandinavia, Galaxy in Australia, Shiniwatra in Thailand, as well as other operators in Africa, the Middle East and Greece.

My prime focus is on Conditional Access and cryptographic security for Pay TV with secondary emphasis on emerging areas such as Electronic Commerce and Internet security.

I would describe myself as an applied cryptographer and system designer with large experience in the design and implementation of logic, microprocessor and embedded firmware projects.

When I left I had completed the development of a five-year strategy for Pay TV security. This demands complex analytical and synthesis skills as one has to be able to attack problems in a multi-faceted manner.

In order to give an idea of what this entails I have attempted to break down my current function into smaller chunks.

**Phase 1 - Strategic.**

- i. Customer requirement analysis. This involves both a comprehensive understanding of the emerging business plans as well as a solid understanding of the proposed product(s) and their constituent technology. If the technical discipline is unknown or insufficiently understood I need to reach a solid understanding of its principles.
- ii. Development of detailed threat models. In any secure system one has to identify all possible threats that one can conceive of. Having done so one proceeds to weight each threat as a function of severity of the perceived threat.

- iii. Conditional Access and Security Top level functional requirements. While a customer typically has a good idea of the type of product he wishes to develop security has to be engineered in at the earliest point. In my experience the business plan, technical and security requirements typically tend to modify each other.

## Phase 2 - Design and Specification

- i. Top level security system specifications. Typically these are intertwined with the specifications of the non-security aspects of the product(s). This requires a both a solid technical background in the areas of my own strength as well as the ability to work within a team in areas of my own inexperience. A perusal of the more historical areas of this CV will yield a overview of my areas of expertise.
- ii. Development of key distribution hierarchies and cryptographic protocol specification. I have extensive experience in system design using both symmetric and asymmetric cryptography. A lot of attention is given to both key initialization and operational key cycling and expiration.
- iii. Detailed implementation requirements including all aspects of smart card, chip and system security.

I have spent extensive time with Smart Card chip vendors such as Philips, NEC, Siemens, Atmel, Motorola and others understanding their implementations in detail. This is done with a view to both forming a opinion of physical security (which differs widely from vendor to vendor) as well as being able to specify detailed implementation details for Smart Card firmware and hardware as other security weakness emerge at boundaries between disciplines.

I have extensive experience in ASIC design which has proved valuable as a lot of attention has to be given to testing and initialization of secure silicon circuits.

- iv. Fundamental cryptographic algorithm development. I will typically either select standard one or develop proprietary algorithms. I have a fairly extensive network of world-class crypto-analysts for auditing any proposed algorithm for weaknesses. In the past I have worked with such luminaries as Donald Davies, Jim Massey, John Gordon and Fred Piper. I consider myself far stronger in symmetric cypher design and have designed several symmetric cyphers. I would not attempt to design an asymmetric algorithm, but would feel comfortable in the application of known algorithms.
- v. I am also involved in other emerging products in electronic commerce and the Internet domain but as yet have not actively specified any products that are available in the market place. I have been part of the team that has engineered the initial technology used by M-Web for their data broadcasting system currently being launched in South Africa.

## CHAPTER 4

# LIFE SKILLS

I view myself as an innovative creator of technical business solutions. I typically have a strong product orientation as I feel the result must achieve the business end for which it was designed in an economic manner.

I enjoy creating technical strategies and roadmaps. I get very irritated if people do not plan ahead when they are able to do so; all questions and problems must be faced and adequately dealt with. Procrastination is not an option. When information is unavailable I am able to live with a high degree of ambiguity while the situation clarifies.

In a more formal way I would like to itemize the design skills I possess. It is helpful to break this down into sections. The sections are not disjoint as I view the hardware as an integral part of the microprocessor design as I typically craft hardware accelerators for microprocessors. This involves careful system design to partition functionality between hardware and software. In fact I model a microprocessor as nothing more than a re-programmable state machine! Further to this I have been involved in the actual design of microprocessors although I would not rate myself as expert here.

I have managed my own company since 1998. I have had as many as 16 development engineers under my control. During this time my company has implemented several successful projects and products. I have designed and managed the implementation of large-scale technical projects. In order to do so I take a System Engineering approach as I cannot manage without understanding the technical reasoning. This is especially critical in security engineering.

My main design skills are Cryptographic Systems and VHDL based logic development.

### **Cryptographic:**

- i. I am able to apply cryptographic concepts to solve business problems. While I have developed symmetric algorithms which have gained international acceptance I do not view myself as a cryptographer but rather an engineer with a few cryptographic inclinations.
- ii. I have a very firm grasp of applied cryptography. I find myself able to quickly spot weaknesses at a system level in security systems. Further I find myself able to easily and quickly evaluate security constraints

and risks within all aspects of engineering. I am fully aware that security loopholes in systems typically occur at the systems level rather than in the cyphers. I am further aware that often it is the implementation details that surround good cryptography that often produce loopholes. Hence auditing of designs and their methodology is an essential if onerous task.

- iii. The apparent complexity of cyphers and abstract cryptographic concepts do not prevent me from easily seeing weakness and ways of solving them. My extensive Integrated Circuit experience enables me to evaluate security at a silicon level. Deep-sub micron geometries is not a mystery that prevents me from conceptualizing the risks. Extensive interaction with the TNO in the Netherlands and Smart Card vendors has given me confidence over the years that my ideas are sound.

### **Hardware design:**

- i. I have extensive experience in the design of Integrated Circuits for consumer equipment in the field of Pay Television Conditional Access. A typical design process would be to model the operation of the circuit in 'C' and then having completely understood the functionality then move to the hardware design phase.
- ii. I would rate my knowledge of VHDL as expert. In order to implement complex logic designs right first time one must operate at a higher level of abstraction. I am able to write VHDL code for synthesis as well as for test benches. I design extensive test benches using a composite of VHDL and 'C' for test vector generation. In complex designs it is imperative that one automate the checking process. This allows one to accurately validate the design.
- iii. I have used many synthesis tools. I have extensive experience of the Viewlogic Silcsyn tool used for ASICs and Galileo from Exemplar used for FPGAs. Lately I have used the Altera Quartus software for all my FPGA development. I have spent vast time optimizing VHDL code styles for optimal synthesis to achieve small and fast designs in conjunction with the configurability of the synthesis tool.
- iv. I have a good working knowledge of most FPGA families. I would rate my knowledge of Actel and Altera Stratix, Cyclone and 20K the best. I have extensive experience of synthesis and place and route for FPGAs.
- v. I have used many simulators. The one I definitely prefer is the VHDL simulator available from Model Technologies in Beaverton. This product has bought by Mentor Graphics and while they have tried to alter it to make it a 'true Mentor' product it remains a good (but much more expensive) product.
- vi. I am an ardent believer in VHDL based system level test bench methodology. Within CypheRix I have spent significant resources on developing test tools and test methods which lever this kind of

thinking. This can be seen in the test system developed for BetaResearch.

### **Software and Embedded Microprocessor Design:**

- i. Due to the consumer orientation of my design experience with the focus on Smart Cards I have extensive knowledge on 8 bit processors. I have knowledge of the Intel 8051 family including detailed knowledge of the secure 8051 based Dallas processors. I have designed decoders with the TMS370 family. I have good knowledge of the Motorola 6800 family.
- ii. As most of my design experience was some years ago and given the extremely restrictive memory requirements all of my projects were written in assembler. It is my firm opinion that all security critical functions should be written in assembler. I have repeatedly identified major security loopholes due to designers not being familiar with the CPU they were using as a result of using high level design tools. This is made worse, as often designers do not really know what the compiler is doing.
- iii. I am an ardent fan of implementing a security design in 'C' first in order to test one's understanding of the required design. This allows one to develop the required concepts completely prior to entering the detail assembler coding phases. I believe in creating automated test systems prior to entering the assembler phase. This is then used to test both the 'C' model of the desired design and the final assembler.
- iv. I have experience in emulator design as often I had to design a hardware accelerator for a microprocessor. This therefore requires one to create the functionality in an FPGA inside an emulator in order to be able to write the final code for chip manufacture.
- v. It must be stated that I do not rate myself as a current software developer although I can program, I do prefer cryptographic systems and logic design.

### **Broadcasting:**

- i. My main function was as a system engineer. I was involved in network planning and test and measurement.
- ii. I had extensive knowledge of test equipment for video quality and RF measurement. As I have not been active in the field for 5 years I would suggest that my knowledge is somewhat dated although the concepts will still be sound.
- iii. I would rate my systems knowledge of MPEG as expert. I played a large role in the standardization of MPEG2 Conditional Access systems.
- iv. I have extensive knowledge of analogue PAL and NTSC broadcasting.

## CHAPTER 5

# PATENTS

Currently I hold several. As often the formal name of a patent gives little idea as to its real use I have elected to give a brief description. I do quote the patent number should someone wish to read further.

### PATENTS FILED AND GRANTED

- i. The Block cipher used in the European Digital Video Broadcasting standard is largely based on a cipher I developed using large S-Boxes. The concept of Reverse Cipher Block Chaining was derived in order prevent the fixed Elementary Stream Headers, i.e. often repeated known plain text, from being used in crypto-analysis. (European Patent EP 0 723 726 B1)
- ii. A mechanism to allow a Integrated Receiver Decoder or Conditional Access Module to verify that the smart card in operation is in fact a valid Irdeto one. It is superior to the zero knowledge Fiat Shamir protocol in that it is not vulnerable to a fork attack., which is where a legitimate smart card is used for the verification process but a foreign one is used to decrypt the incoming encrypted control words. (International Patent Number WO 97/38530)
- iii. A mechanism whereby a Integrated Receiver will only work with legitimate satellite transmission approved by the system operator who put the decoder in the field, thus protecting this operator's investment. (European Patent 750423)
- iv. One of the fundamental problems of conventional Smart Card technology has is that it cannot defend itself while un-powered. Given that battery technology on Smart Cards will mature in the next few years there is a golden opportunity to create a technology that can always defend its secrets. Secondly, most chip technology in the past has attempted to secure the entire device often with a lot of complexity. This makes it difficult to defend, as there are many possible avenues of attack. The concept patented is a cryptographic co-processor where one puts the required secret key(s) and strong cryptographic algorithm encapsulated inside a cocoon of power and sense wires, which allows keys to be cleared when an intrusion is detected. This results in a simple system, which is simple to audit for soundness. (European Patent EP 0 893 751 A1 – Application Number 97202854.2)
- v. A method for using a small low speed device (such as a Smart Card) in conjunction with a high-speed bulk decryption device (such as a decryption ASIC) where one can lever the security features of the small slow device to the large fast one. This allows the design of a system with significantly higher bandwidth with a high level of

security. The technique made a novel use of error propagating cipher block chaining. (European Patent EP 0 984 630 A1 Application Number 96202916.7).

- vi. A mechanism for identifying the Smart Card that has been used to create clones (pirate Smart Card). Part of the detection method either ejects them from the functional set or makes it simple to later eject the clone root Smart Card. (European Patent EP 0 984 629 A1, Application Number 98202914.2)
- vii. A method of storing keys in a more secure method in a Smart Card. This method forces a person doing a physical attack (such as using a focused ion beam) to have to analyze a much higher number of different points on the integrated circuit design. This scheme makes use of cryptographic shares in a novel manner. (European Patent EP 0 923 124 A1).

## CHAPTER 6

# 12 YEARS IN M-NET / IRDETO

I have decided to split up my time with M-Net and Irdeto into three sections as the job functionality altered significantly in the differing phases of the companies' life. I actually view them as three different jobs as I had to learn vastly differing skills to be able to achieve the design goals.

### THE EARLY YEARS

I joined M-Net in April 1986 when all they could offer was a huge challenge and three month's salary. I became one of three people who had to set up the transmission side of the operation. Jock Anderson and those under him were responsible to everything from the studio out. This included microwave links to transmitter sites, encoding equipment, the overview of the SABC's transmission functionality, design and manufacture of Decoders and the personalisation thereof.

In this time I was primarily involved in project management and broadcast engineering. I ran the entire network from the studio outwards single-handed for several years.

A significant part of this function was the project management of the Video encoding equipment, which was done in conjunction with the LGI at the University of Pretoria. I oversaw the design team there and assisted them from a broadcast perspective to convert over from the American NTSC standard to PAL.

This period was characterized by doing anything required to make the operation a success. Often we found ourselves doing things for which we had little or no training at all, just go and do it! I look back on this time in a very unique way as one was part of a small band of people who took on a huge task and made it happen.

### THE ANALOGUE ERA

The move from management and network operation to design was the result of a unique opportunity, bearing in mind that as a broadcast engineer had little or no background in digital design aside from lecturing basic logic theory at Technikon. The early analogue decoder had a unique design fault. It would change its address in the presence of power transients. Staff members of the LGI (A professor and a doctoral student)

were unable to isolate the fault after a month of effort. I requested a opportunity to investigate and was given permission to do so in my own time! I tackled the fault from a very different perspective and focused on being able to replicate the fault prior to investigating it. This allowed me to proceed a step at a time as I had to first learn how to use a logic analyzer and build up my rudimentary knowledge of microprocessors and assembler programming. Within a week I was able to identify and rectify the fault.

This led on to being given the task of re-designing the firmware inside the analogue decoder. This was indeed a milestone in my career as I embarked on a whole new phase of self educated endeavor.

In the next five years I implemented the following projects:

- i. I redesigned the microprocessor firmware of the then current analogue decoder. This was primarily a learning curve for me and enabled M-Net to gain (incremental) in house design expertise.
- ii. In the course of this I began to identify security weaknesses in the current design. This lead to M-Net being the first Pay TV design in the world to use internal EEPROM for the secure storage of keys. We were the first user of the TMS370 in Europe. We managed to convince Texas Instruments to let us use their emergent technology in a very early phase.
- iii. During this time I re-engineered the video encoding equipment. While I wanted to totally redesign the device time did not allow this. I had to limit myself to improving the firmware in the microprocessors. This was done with a view to being able to sell complete Pay TV systems on the open market.
- iv. In the following years I re-designed all the firmware for the decoders, encoders and personalisation equipment for the new markets almost single-handedly. I designed new and ever more secure systems for Italy, Benelux, Africa System 2 and Greece. This phase was still characterized by a few men trying to achieve great things with extremely limited budgets. One just could not expand the team, remember that M-Net was only just cash positive at that time.
- v. I specified three custom TMS370 devices that Texas Instruments implemented for use by M-Net. The nature of these changes were either in improve security, to customise IC packages and pinouts and to add functional elements we needed. To date I have some 1.5 million microprocessors in the field of my designs.
- vi. The transition to the digital era was a complex one. I was part of a design team that designed the third generation of analogue Pay TV. This was a very secure system with two inter-linked secure components viz.: a Smart Card and a key based descrambling ASIC. I was responsible for the cryptography and CA part of the system design. It never saw the light of day as the digital era dawned. However it played a pivotal role for us as I was able to show how one could take the Smart Card half of the design and re-use it for the

digital system. By this time others had taken over the actual implementation from me.

- vii. Other interesting projects included a prototype line cut and rotate and line shuffling device. This was used to investigate how we could improve our video security. It was deemed too expensive in the light of the emerging digital devices.

## THE DIGITAL ERA

- i. I was the first engineer in the company assigned to actually begin an implementation for MPEG Conditional Access. I spent most of the first half of 1993 touring the world learning about MPEG and deciding on how to secure it. It was a phase of extensive system design. During this time I helped lay the foundation of the current Irdeto digital system. I specified all the core cryptography and did the initial CA system design. The symmetric decryption and authentication algorithm in the smart card are my design. This included the receiver, conditional access module, smart card and scrambler.
- ii. I lead a team in the UK at the offices of NTL (today NDS). I had for several years wanted to design logic circuits and ASICs so, I moved out of a management and the system design function to learn VHDL and to design ASICs.
- iii. I specified the first descrambling ASIC for others to implement. Its functionality included a proprietary block cypher (known as "Fast") and the Conditional Access data filter required to extract received entitlement messages for a high-bandwidth data stream. This involved a lot of interaction with the designers of the conditional access module and smart card in an advisory capacity. If there is one single thing I criticize myself on here, it was in underestimating the amount of ongoing system engineering required. This was clearly influenced by my desire to enter the logic design arena. One must learn by ones mistakes.
- iv. From there I specified and built the VHDL and 'C' composite test bench which tested the chip design as implemented by Nanoteq. I was able to identify critical design faults and played a significant part in Irdeto being able to produce the first MPEG CA descrambling device in the world right first time.
- v. While the chip was in manufacture I designed the 'Fast' scrambler to fit inside the NTL multiplexer. This included interface specifications between NTL and Irdeto. I won a design award for this design as it was the first significant design for FPGA technology done in South Africa using VHDL.

- vi. I then joined a team to design and build a DVB compliant descrambling chip. I specified the DVB compliant Irdeto CA filters and implemented the descrambling and MPEG interface circuitry for the DVB compliant descrambler chip. My first ASIC! I designed the test bench for the entire chip and was able to repeat the creation of a usable chip first time (there were a few logic bugs which were benign). Subsequent phases of the design rectified these errors. To date there are more than a million euro-chips in the field.
- vii. I specified the entire DVB scrambler design including conditional access interfaces, multiplex functionality with respect to CA messages, logic, cypher and authentication functionality. This was done for two multiplexer vendors viz NTL and a US based company called TVCOM. I proceeded to design the logic FPGA based elements for both vendors. This enabled Irdeto to have the first DVB compliant CA system in the world on air in Germany.
- viii. I had extensive involvement in systems specification of several CA descrambling projects in later phases of the digital process. This included the next version of stand alone descrambling technology which involved crafting custom RISC cores and marrying them to descrambling circuitry. I have also been involved in embedding CA in standard MPEG chips sets from SGS, NEC, LSI and VLSI.
- ix. My latest major implementation project was to design and build a stand-alone scrambling device to allow Irdeto to be independent of multiplexer vendors. This is a major piece of MPEG equipment with allows the headend Conditional Access Control system to directly inject messages into and scramble MPEG2 transport streams. This involved extensive system engineering, and building up and leading a team of five logic engineers. This involved extensive mentoring and education as experienced resources were unobtainable.
- x. I then moved over to the systems group as I was extremely concerned to begin the next generation of conditional access technology, I felt it as paramount that Irdeto has a ready solution for a smart card security upgrade when piracy occurs. So I made the difficult decision to move to full-time Conditional Access system design and specification. This was made extremely difficult, as the hardware team I had built up were (and still are) an extremely good bunch of people to work with.
- xi. Since leaving Irdeto I have done more VHDL based logic development for them. I have implemented the descrambling and filter elements in the Samsung mobile phone for mobile Pay TV in Korea.

## CHAPTER 7

**REASON FOR LEAVING M-NET /  
IRDETO**

Over the last eight years the M-group (i.e. the companies that were spawned out of M-Net) have been setting up a technology house in the Netherlands. Management felt that this lead to non-optimal operation of the design and support functions.

Management decided to consolidate the design functions in the Netherlands. Although I was made a good offer to go to the Netherlands in my then current capacity, I do not see my way clear to go. This is primarily due to family reasons as I value the input the greater family has to make in the lives of my children.

Hence it is with deep regret that I elected to take retrenchment.

## CHAPTER 8

# EARLIER EMPLOYMENT

### 1979 - 1983 SABC

After National Service I joined the SABC in Bloemfontein as a Learner Technician. I was fortunate in being able to go to Technikon Witwatersrand for two years to obtain a T4 in Broadcast Engineering as part of a five year employment contract.

I worked a Head Office Transmitters for three years. I view this phase as my real introduction into engineering. People like Jock Anderson took time to teach me and to broaden my horizons. I specialized in test and measurement of broadcasting systems. This included field strength measurement, spectrum analysis, time-domain instrumentation (i.e. oscilloscopes), RF transmission line measurement, power measurement, and frequency measurement.

I also installed various transmitters and receiver equipment.

### 1983 - 1984 SA PHILIPS

I spent a brief time of nine months a SA Philips in Wadeville doing project management with some design work. I found that the then company style of operation problematic as often I was given design tasks which were impossible given the time and budgetary constraints.

### 1984 - 1986 TECHNIKON WITWATERRAND

I lectured at Technikon Witwatersrand for two years in the field of Broadcast Measurements and basic digital electronics. It must be borne in mind that the logic I taught was at a T1 level and that this was in the early 1980s. So things were quite different to today.

I thoroughly enjoyed being able to help people help themselves. I derived a lot of satisfaction from the people contact both with students and other members of staff.

I only left the Technikon because of the interesting opportunity afforded by M-Net.

## CHAPTER 9

**PERSONAL DETAILS**

Date of Birth	25 July 1959
Place of Birth	Harare, Zimbabwe
Marital Status	I have a super wife Sue, whom I married in 1982. We have three adopted children Rachel (16) and Tamaryn (12) and Timothy (9) (known as MOD – Master of Disaster).
Residence and Office	66 Westmoreland Road, Kensington, Johannesburg.
Hobbies	Scuba Diving (BSAC), bird watching (feathered kind) and astronomy.
Tertiary Education	Diploma in Broadcasting Engineering (old T4)
Schooling	Matriculated in 1976 from Saint Stithians College in Randburg with university exemption.
Military	1 South African Infantry Battalion and 5 Signal Regiment. Currently non-active Lieutenant

: