Secure and trusted Femtocells

Technical White Paper

June 2011

Picochip Ltd

Upper Borough Court
Upper Borough Walls
Bath BA1 1RG
UK
+44 1225 469744
www.picochip.com

Contents

Executive Summary

Femtocells have emerged as a key enabler of future communications network development. More than a useful add-on that delivers better service to the consumer and increased revenue to operators, they are also an essential part of future network architectures.

The concept is simple: making a basestation cheap enough to be deployed in high volume for residential use, connected to the core network via broadband. This can deliver to a subscriber the same service and benefits as a fixed-mobile convergence (FMC) offering such as voice-over-WiFi, but using existing standard handsets.

Moreover, the use of femtocell architectures can help to surmount many of the technical challenges that have become evident as operators deploy 3G networks: and that look set to worsen with the advent of 3G Long Term Evolution (LTE) and WiMAX.

These are challenging times for mobile operators: many markets are approaching saturation; price competition is intensifying; new competitors are entering the market, often as mobile virtual network operators (MVNOs) with attractive cost structures and powerful brands.

In some markets carriers have problems with coverage: this is a major cause of customer dissatisfaction and churn. In addition, operators face ‘the bandwidth tsunami’ as usage explodes, but revenues are squeezed

Femtocells provide many of the answers delivering capacity and coverage exactly where needed, but challenges remain in their deployment: network integration, security, provisioning, radio interference and the like. However, these can be solved.

One of the key issues has been the cost of the femtocell. Low-cost hardware is critical to make the business case viable. Once more, this is now realistically achievable.

The benefits to the consumer include better coverage, clearer voice connections, better battery life, faster data rates, cheaper calls and the great convenience of using a single handset. The benefits to operators are measured in increased average revenue per user (ARPU), reduced churn and increased customer loyalty.

However, femtocells potentially open up a number of very serious security concerns. There are risks that eavesdroppers could intercept cellular traffic, while carriers have worries that an attack could use femtocell as an entry to their core network. These concerns have all been addressed and femtocell security is strong: this paper explains the techniques used.

1 Introduction

Only a few years ago, the idea of a cellular basestation in the home would have seemed impossible, especially given the public perception of a basestation: never enough of them to make a call, but not something that should be seen. The reality today is very different, with the industry moving to extremely low-power home basestations, or femtocells, the same size as existing in-home wireless equipment. These small devices have a low price tag to match: they are affordable as consumer products in themselves, and present an economically viable case for operator subsidy.

Over 17 femtocell deployments have now been rolled out globally, with many more operators expected to join them by the end of this year.

Femtocells are in fact still a relatively new technology. The first developments and prototypes were on show at conferences in 2007, but real products have only been available since 2009. Roughly speaking, the technology 'arrived' in 2007. The bulk of the technological issues were solved in 2008, these being mainly the development of the Iuh standard for connection; proof that interference was something that could be solved and proof that femtocells would not ultimately break the macro network). The first trial; ("friendly customer") launches were in 2009, but there was still work to do on productizing, this being sorting out OSS/BS, provisioning, billing and other "boring but essential work". Those issues are all now solved and as a result carriers have been shipping in high volumes.

The technology behind femtocells is far from trivial. Operators have approached their deployments carefully, ensuring they "cover all bases" to give consumers confidence in the solution. But long before the deployment stage, companies in the femtocell ecosystem were working hard on overcoming the substantial technological hurdles involved.

Femtocells actually include far more intelligence than traditional basestations. Because of this change in the way tasks are partitioned in the network, femtocell chips like the picoXcell family from Picochip need to provide enhanced security features for authentication, location detection, and encryption as well as the prevention of denial of service attacks.

Conventionally, the "Node B" (3GPP jargon for "basestation") is the Radio Stage, while the Radio Network Controller (RNC) handles the intelligence and management. The RNC sets up and tears down calls, controls power levels and session parameters, allocates bandwidth to users, and supports handoff between sectors or cells. It is the bridge between the radio access network (RAN) of basestations and the core network. One RNC can control many basestations but when the number of basestations is to be measured in millions per network this architecture doesn't scale well. In a femtocell, all of this intelligence is localized. Managing calls, controlling interference (which is crucial, so femtocells don't degrade the network by transmitting inappropriately), and interfacing the radio with the broadband network securely all are RNC functions. So a femtocell isn't just a basestation, it also integrates the smarts of the RNC—and a lot more too.

The security issues were not only solved but also provided another reason why femtocell rollouts on an enterprise or citywide scale are more effective than Wi-Fi. To begin with, everything in wireless is secured with strong encryption. There are theoretical attacks. But even GSM, which is an old technology, is still robust against all practical attacks, and 3G is stronger still.

Then there are end-to-end techniques. For example, the core must authenticate the handset, but also vice versa, so it is very hard to intercept. Cellular was designed to be secure in a way that Wi-Fi never was. (There is a value to calls.) Finally, it is hard to eavesdrop or intercept calls if you do not know who to listen to. A perhaps surprising fact is that the phone number is not used. An IMSI number that only maps to the phone number in the core identifies the handset.

This paper addresses the issues facing the successful deployment of femtocells and argues that the technology will play a vital part in future networks and service offerings. The arguments apply equally to 3G and to emerging wireless broadband technologies such as WiMAX and 3G LTE.

1.1 Network Considerations

The Radio Access Networks in use today comprise hundreds of base stations connected to a single Radio Network or Base Station Controller (RNC/BSC). The interface is the Iub running the ATM protocol over dedicated leased line

Accommodating hundreds of thousands of femtocells connected over the Internet raises a number of important questions:

1. Is it scalable?
2. Is it secure?
3. Is it standardized?

A number of different 3G femtocell architectures have been proposed to accommodate the potential increase in home basestations, however one has been adopted by 3GPP as a reference architecture for the evolution to femtocell networks. As such it is the approach most likely to find adoption amongst the W-CDMA community. It defines two new network elements, the Home Node-B (the femtocell itself) and a concentrator type element, the HNB Gateway (HNB-GW). Communication between them is via a new standard interface, Iuh. This network architecture is given in Figure 1

This approach allows functions to be partitioned differently between the Node-B and RNC, enabling the HNB-GW to handle multiple Node-Bs. It fits seamlessly into a mobile network operator's RAN by supplementing or replacing its current RNCs with the concentrator element to service thousands of femtocells.

The Home Node-B (HNB) itself can handle the radio resource management functions formerly residing in the RNC. The HNB-GW aggregates traffic into the existing core network. Amongst other things, the Iuh interface provides important security functions, control signaling and a new application protocol (HNBAP) designed to ease HNB deployment.

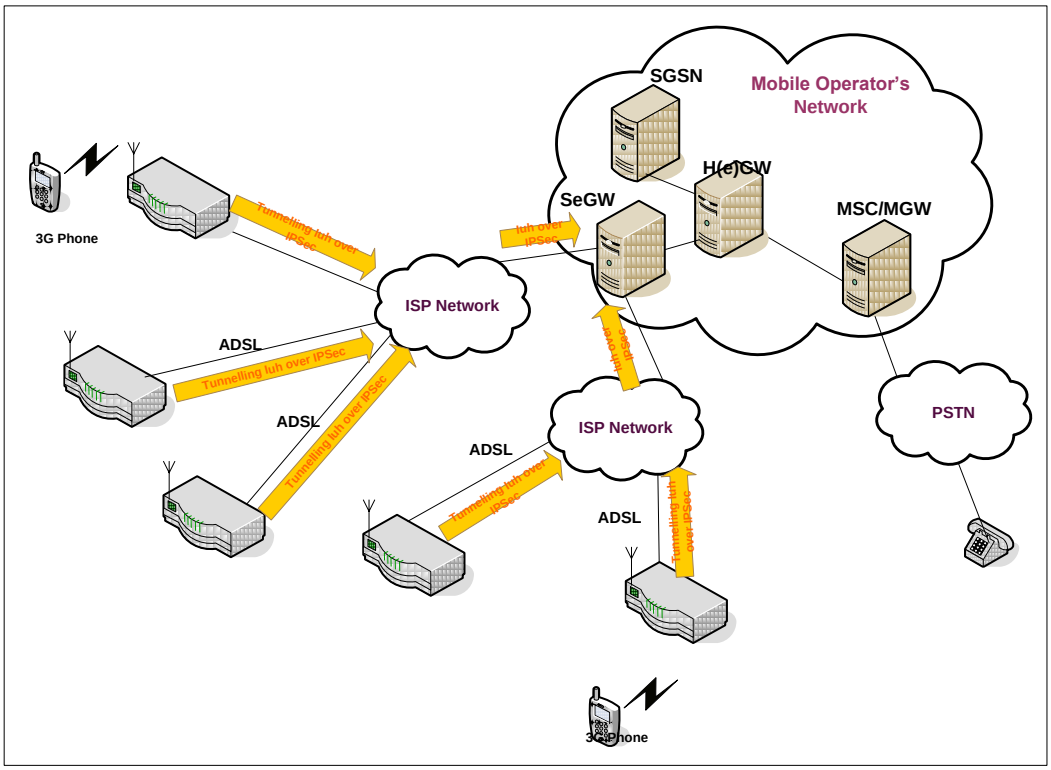

Figure 1: Concentrator/RNC (HNB-GW) using Iuh

1.1 RF Considerations

In the early days observers had questioned whether the deployment of large numbers of femtocells would create insurmountable RF management problems. However with some intelligent design by equipment and semiconductor manufacturers – as well making use of some of the inherent benefits of the femtocell approach – it has proved possible to allay these fears.

1.2 Synchronization

3GPP specifies that basestation transmit frequencies must be very accurate and closely synchronized, requiring precise clock references. For larger basestations the accuracy is 0.05 parts per million (ppm), although this has been relaxed to 0.1ppm for picocells in Release 6 [] and 250ppb (0.25ppm) for femtocells in Release 8. There have been proposals that future versions of the standard, or even operator-specific waivers, would relax this constraint.

For a low-cost femtocell implementation, implementing such synchronization starts to become a significant part of the bill-of-materials (BoM) making alternative solutions vital. In fact, the constant pressure to reduce basestation costs, whatever the equipment size, has meant that lower-cost synchronization solutions are considered. The most common is NTP (Network Timing Protocol) although there are alternatives. These include IEEE1588 and GPS as well as using innovative, low-cost/high-stability TCXOs.

1.3 Provisioning

Just as consumers are able to buy and successfully install a WiFi access point in the home, installing the femtocell must ideally be the same: seamless and without the need for on-site assistance. But unlike WiFi, which in its simplest form is a standalone network, the home basestation must be detected and integrated into the overlaying mobile network – all without user intervention with a high level of security to prevent fraudulent use.

Registration and authentication may be carried out using the same techniques as are used by many cable and ADSL network operators. Indeed, a standard already exists for the remote provisioning and management of DSL gateways (TR-069) which this has been extended (TR-196) to include specifics for femtocells.

2 Low-Cost Implementation

In the past, equipment cost has been a major hurdle for in-home communications, but advances in technology and performance are now opening up new possibilities. In fact, the approach to the femtocell has more in common with handset design than a basestation. And, like handsets, having the ability to provide software upgrades is becoming increasingly important as standards evolve and enhancements are made.

In fact, femtocells are very cost-effective. In many respects they can be made more cheaply than a handset. Although the baseband is more complex, there is no need for the expensive color screen or battery; power constraints are less stringent, and there is no need to use the most costly, miniaturized manufacturing techniques.

Figure 3 shows the Picochip PC8208/PC8209 femtocell software reference design. At the heart of the design is one of the company's latest multi-core DSP chips: the PC323 [2]. As well as the proven picoArray – multiple DSPs interconnected by a high-speed bus and programmable switches providing a fully deterministic processing core – new functionality has been integrated to meet the needs for improved performance at lower cost.

As well as a number of dedicated hardware function accelerators (HFAs), the device includes an embedded ARM1176JZ-S core [3] that reduces external chip count. This means the PC323 lends itself well to low-cost solutions such as the home basestation.

A unique feature of this architecture is that the bulk of the functionality is in software running on the PC323. All of the 3GPP baseband processing is coded on the picoArray, while all of the control functions and higher-layer processing are on the ARM core. The two software environments are integrated onto the same device and booted from one Flash memory. Upgrades are therefore a straightforward software change, and can be performed remotely over the Internet connection.

The Picochip WCDMA reference design is compliant with the 3GPP Release 8 specifications [4], and delivers 42Mbps high-speed downlink packet access (HSDPA) shared by up to 32 users. It implements all of the required baseband processing (including sample rate, chip rate and symbol rate operations), as well as MAC-hs scheduler, operations and management (OAM) functionality and protocol termination.

An Application Programming Interface (API) supports the exchange of internal data and control messages between the picoArray and the ARM core. Figure 3 shows the protocol stack and breakdown of functions for a Iuh network architecture. For the microprocessor this includes the network interface software and Operations and Maintenance (OAM) functionality.

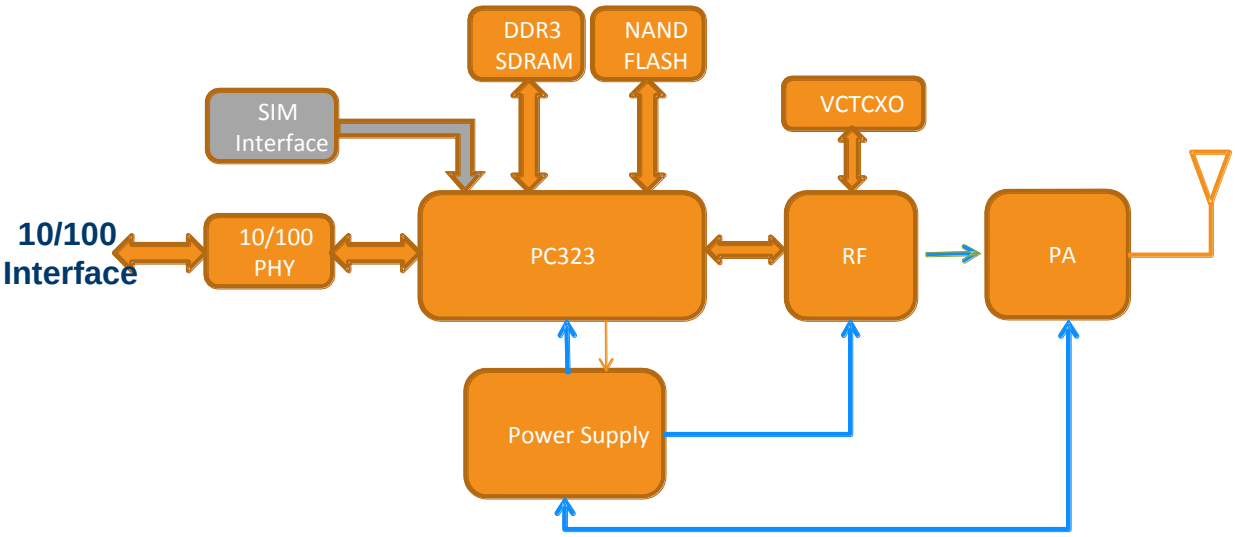

Figure 2: Standalone Femtocell with Ethernet interface

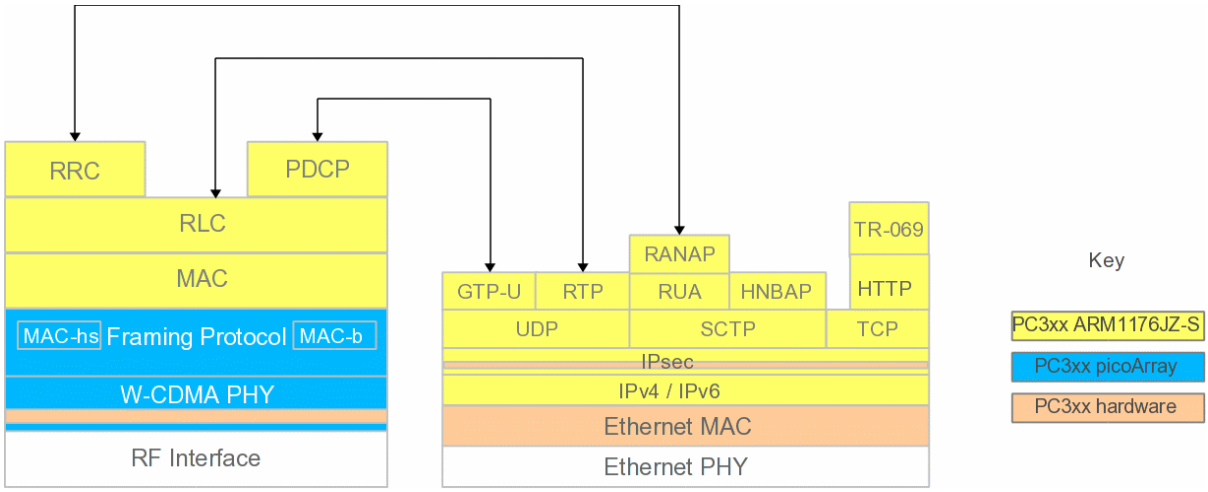

Figure 3: Network Interface, NBAP and OAM support

3 Security

Driving the acceptance of femtocells has been accelerated by the formation of an industry body - the Femto Forum. This organisation has been set up to enable and promote femtocells and femtocell technology worldwide. The Forum is chartered to encourage the growth of a partner ecosystem committed to innovation in standards-based network infrastructure and to achieve high levels of collaboration and product interoperability. Some of the work carried out by this forum has been accepted by 3GPP and this has been published as technical specifications. One such document is TS33.320, which specifies the security of "Home node B" and "Home evolved node B" ” (the 3GPP terminology for HSPA and LTE versions of femtocell aka H(e)NB). In this specification a number of threats have been identified which the providers of femtocells must address. The solutions need to be such that the BoM is still as low as possible. In other words, addressing the identified threats and indeed others need to considered as part of the main femtocell device.

The specification identifies a number of security requirements and principals and also details a series of security features. In particular, the specification defines a Trusted Environment (TrE) needed to perform sensitive functions and store sensitive data. This data must be unknowable to unauthorised entities.

- The TrE must be built from a hardware root of trust
- The Integrity of the TrE must be verified during the boot process
- The TrE must verify the integrity of the rest of the system software
- The TrE must perform the required sensitive functions to validate the device and device integrity
- The TrE must perform the required sensitive functions to authenticate the device with the operator network.

This section provides an overview of the approaches Picochip has taken in order to address not only the identified threats in TS33.320, but also the threats in the manufacturing chain of the femtocells. Instead of Picochip employing specific silicon hardware for all the threats, and hence increase the cost of the femtocell solution, it has adopted the more flexible approach of utilising ARM's patented system wide security, TrustZone® technology, in addition to simple, generic hardware on silicon to provide the required Trusted environment.

Using this in conjunction with a secure root of trust boot strapping mechanism, ensures a secure and trusted system.

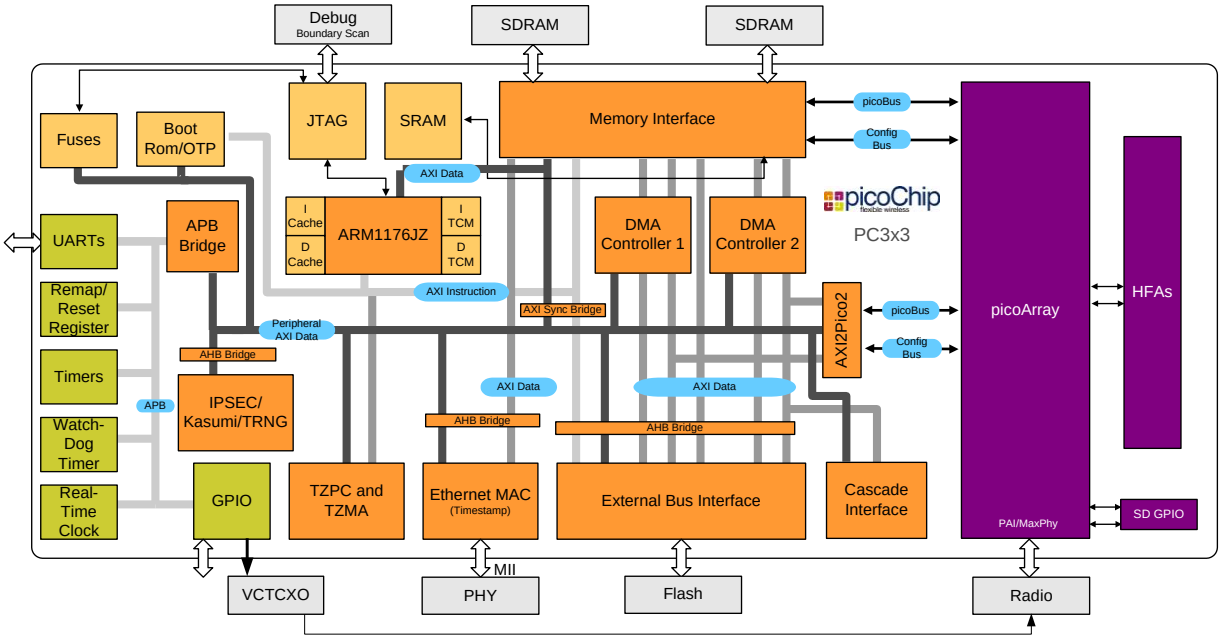

Figure 4: PC323 picoXcell device

Figure 4 shows the major blocks within the PC323. In particular it shows the internal boot ROM, Cipher engines, e-Fuse and SRAM. These are used in conjunction with the ARM TrustZone technology to create a secure and trusted system.

In the following sections a number of security aspects are highlighted and solutions used by customers are given.

3.1 TrustZone Technology

ARM TrustZone technology is an integral feature of the ARM1176JZ-S™ processor and was introduced through the ARM Architecture Security Extensions. These extensions provide a consistent programmer's model across vendors, platforms, and applications while providing a true hardware backed security environment.

TrustZone is the set of architectural security extensions found in many of ARM's newer, such as the ARM1176JZ-S and Cortex™-A series processors which partition a system-on-a-chip's (SoC's) hardware and software resources into secure and normal worlds. The Secure world is used to provide the Trusted environment (TrE). The normal world is used for everything else. The hardware logic in the AMBA®3 AXI™ bus fabric ensures that resources marked as secure cannot be accessed from the normal (non-secure) world enabling a strong security perimeter to be built between the two.

The security extensions provide a set of well defined mechanisms to transfer control between the two worlds in the CPU core allowing it to perform both secure and normal functions in a time-sliced fashion removing the need for a dedicated security core.

The CPU core and the bus interconnect use a non-secure (NS) bit to indicate the origin of any request and only permits accesses from the secure world to secure resources to complete successfully. An access to a secure resource from the normal world will result in an abort and the secure world may access both secure and normal resources.

Extensions in the virtual memory system allow memory regions to be marked as non-secure such that both worlds may share cache lines to maintain coherency and achieve high performance shared memory communication.

A new operating mode "monitor mode" is introduced to the core to permit switching between secure and normal worlds. This mode always runs in secure mode and can be entered by the new Secure Monitor Call (SMC) instruction, and the IRQ, FIQ, external data abort and external prefetch abort exceptions. The SMC instruction always traps to the SMC vector and the behaviour of the other exceptions can be configured by software depending on the system software design. The monitor mode software will typically save the state of the current world into secure on-chip memory and load the state for the other world. This is typically an inexpensive operation and only consists of saving the general purpose registers for cores without additional coprocessors such as a VFP.

A range of peripherals are available to secure a system including the TrustZone Protection Controller (TZPC) and the TrustZone Memory Adapter (TZMA). The TZPC is a configurable controller that marks peripherals on the AMBA3 AXI bus as being a secure or normal peripheral which in turn controls the protection signals on the bus to prevent the non-secure world from making accesses to secure peripherals. The TZMA allows on-chip memory to be partitioned in to secure and non-secure regions allowing secure software to run entirely on-chip without allowing accesses to the normal world but still reserving a portion of on-chip memory for the normal world. The TCM's (Tightly Coupled Memories) may also be marked as secure or normal and can be a valuable resource for implementing a secure software system.

Picochip's picoXcell family of devices incorporate the TZMA and TZPC so that the chip can be partitioned into secure zones depending upon the operation being performed and where in the manufacturing or provisioning chain the femtocell is.

All of the peripherals shown in Figure 4 can be configured to be in the secure or non-secure zones. This includes the internal SRAM, where regions can be in secure or non-secure as well as the picoArray itself.

3.2 Secure boot

The picoXcell devices from Picochip have a secure boot mechanism which ensures the device uses the on-chip bootrom and the security features within the device. In addition to the bootrom there is an e-fuse and also an OTP block. The efuse macro is used for informational and control operations.

At reset the device enters the bootrom which determines whether the system is to be decrypted and authenticated before control is passed to the application code. It also determines where the next level of the bootstrap is obtained, e.g. flash or MII. The bootrom, creates the first link in the chain of trust, makes use of the e-fuse block to obtain the secret information to decrypt and authenticate the subsequent next level of bootstrap. The on-chip cipher engines are used to perform the authentication and the bootrom clears up any memory used by it prior to transferring control to the next level. This ensures no leakage of secret information takes place.

The e-fuse also has the facility to control access to certain parts of the PC323, for example, the fuse block can be programmed to disable intrusive and non-intrusive debugging of the ARM. This ensures a potential attacker cannot gain access to the secret information stored in the fuse block.

Should the customer require a different authentication or bootstrap mechanism the PC323 can be configured to jump directly to OTP. In this case the customer specific code residing in the OTP would be responsible for authentication of subsequent bootstraps and establishing a root of trust.

This process can be repeated over more iterations to bootstrap more complex software systems before switching into the normal world preventing malicious accesses to the secret data.

3.3 Untrusted CMs and ODMs

In most consumer markets, devices are manufactured in high-volumes by third party companies. These may be Contract Manufacturers (CM), who only manufacture according the supplier’s design, or ODMs (Original Design Manufacture) who integrate both design and manufacture.

These organisations will have access to information, including copies of code and potentially access to keys (if those are to be blown into OTP during manufacture) and as such are a potential security vulnerability.

To protect against this, information is partitioned and controlled so that even if the CM / ODM does leak information it is not sufficient to compromise the security of the device as a whole.

The device will boot securely from the internal ROM and load the second stage of the bootstrap into internal SRAM. The internal ROM will authenticate the loaded bootloader and if successful will start to execute it. The code loaded will provide a secure monitor which will relocate itself into the TCMs of the ARM1176JZ-S. The code will check whether a public key is already present in the e-fuses. If it is then subsequent code is authenticated using this key. Otherwise the monitor code will program the public key into the e-fuses.

Once these operations are complete the device is ready to perform any of the OEM defined actions as all subsequent code will be authenticated using the OEM's public key and therefore deemed secure.

3.4 Prevention of unauthorised baseband software

In certain regions of the world an OEM may wish to prevent a particular SDR from being loaded in the picoArray. There may be many reasons for this ranging from immature SDR to value proposition of higher specification baseband.

By making the loading of the picoArray's SDR the responsibility of the secure monitor this cannot happen. All requests by the normal world software to load the SDR will go through the hypervisor which will authenticate the baseband image prior to downloading onto the picoArray. If this authentication fails the picoArray will not be loaded.

3.5 Use of TrustZone to provide digital certificate authentication

As shown in Figure 5, the H(e)NB connects to the core network through the Security Gateway (SeGW) over an insecure connection and both parties must be authenticated and communications secured. To prevent unauthorised H(e)NBs from connecting to an operators core network, each device can be provisioned with a public/private key pair and the SeGW's certificate and public key along with the root certificate(s) of one or more certificate authorities to establish a chain of trust. This data is stored in the H(e)NB in secure storage such as OTP or eFuses that are only accessible to the TrustZone secure world and can be generated on the device at time of manufacture such that the private key never leaves the device.

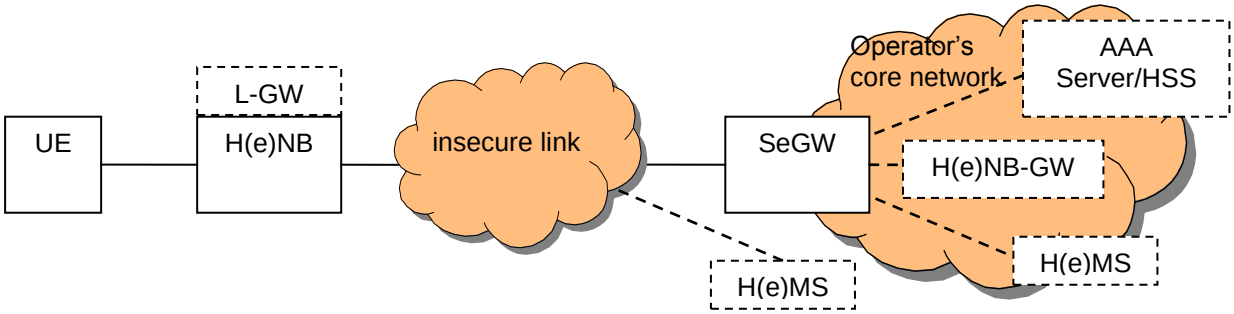

Figure 5: System Architecture of H(e)NB

The authentication of both the H(e)NB and the SeGW can be established by using certificate based authentication to construct an IPSEC tunnel using IKEv2 that will later provide the confidentiality and integrity of the communications between both parties. During the authentication phase the H(e)NB is required to sign the authentication data of the IKE_AUTH request using the H(e)NB's unique private key. In most H(e)NB's the IKEv2 daemon will be running in the nonsecure world of a TrustZone enabled system to leverage the full IP stack of a rich, unmodified, operating system such as Linux and as such cannot be trusted with the H(e)NB private key. To perform the signing operation, we can use

TrustZone to pass the data to be signed over a well defined channel into the secure world where the data can be signed and returned to the nonsecure world without leaking the key.

To implement the signing process the H(e)NB has a lightweight hypervisor running in monitor mode that is responsible for performing the switch between secure and nonsecure world and use the Secure Monitor Call (SMC) instruction to provide entry into the secure world from the rich OS. An ABI between the secure and nonsecure world is defined using general purpose registers to pass a call identifier and optional parameters which may utilise shared memory to transfer larger amounts of data. The SMC call traps to the monitor mode SMC vector and the monitor mode transfers control into the secure kernel which decodes the call identifier and runs the appropriate handler. To perform the signing, the secure kernel validates the address of the payload and copies it into secure onchip memory to prevent any possible race between the request and sampling of the data during the ciphering process. The secure kernel retrieves the private key from OTP memory and then may either perform the ciphering using hardware offload engines or a trusted software implementation. After the signing process has been completed the secure kernel copies the signature to a buffer supplied as an argument to the SMC call after verifying that this address is a valid nonsecure address and returns control to the nonsecure world through another SMC call.

Optionally, the H(e)NB can use symmetric key cryptography to utilise the external non-volatile storage to provide a larger secure vault to hold certificates and private keys allowing the H(e)NB to handle revoked keys without running out of space in the OTP/eFuses.

This approach satisfies the requirements in TR33.320, which the H(e)NB's TrE shall be used to provide the following critical security functions supporting the IKEv2 and certificate processes:

- The H(e)NB's identity shall be stored in the TrE and shall not be modifiable.
- The H(e)NB's private key shall be stored in the TrE and shall not be exposed outside of the TrE.
- The root certificate used to verify the signatures on the SeGW certificate shall be stored in the H(e)NB's TrE and shall be writable by authorized access only. The verification process for signatures shall be performed by the H(e)NB's TrE.
- The H(e)NB's TrE shall be used to compute the AUTH payload used during the IKE_AUTH request message exchanges.

Through this process the H(e)NB can perform all security sensitive operations without the possible leakage of confidential data whilst utilising all of the services that a rich operating system offers. By using TrustZone we can provide mechanisms to update the cryptographic algorithms being used for the signing and revoke keys or certificates whilst reducing the risk of designing a fixed function system.

4 Conclusions

As can be seen from this paper, the femtocell is a complex system - a condensed version of most of the elements typically found in conventional macrocell base stations and radio network controllers of a cellular network. Normally the elements of an operator's network are not directly exposed to the general public in the manner of a residential CPE so it has been essential to ensure these are free from any potential vulnerabilities that might provide access into the mobile operators network as femtocells are directly connected to the operators core network over the customer's broadband connection. In addition, manufacturers of femtocells need to ensure their products cannot be cloned, or counterfeit versions produced, in order they protect their revenues and reputations.

These requirements must be satisfied in a very cost sensitive market; rapid uptake of femtocells is dependent on aggressive commoditisation of a traditional infrastructure market to enabling various operator business models and tariff options.

The most cost effective approach to providing a flexible and secure system is not to design in a large amount of fixed-function security but rather provide a mechanism by which, under a secure root of trust, the underlying software can make use of low-level and reusable hardware to configure a secure system for the target deployment. ARM's TrustZone technology enables just such a system and the only femtocell devices available in the market today with this capability are Picochip's PC302 and PC3x3 family of devices.

References

1. IEEE 1588 Homepage – http://ieee1588.nist.gov/
2. Picochip Wireless Communications Processors, *"PC323 Integrated Baseband Processor"*, Product Brief.
3. ARM Ltd, *"ARM1176JZ-S System-on-Chip Java™ and DSP enhanced processor"*,
4. 3GPP Technical Specification TS 23.234, *"3GPP system to Wireless Local Area Network (WLAN) interworking; System description"*.
5. Picochip Software Reference Design, *"PC8229 3GPP HSDPA/Release 8 Femtocell Basestation PHY"*, Product Brief.

Glossary

3GPP	Third-Generation Partnership Project	MSC	Mobile Switching Centre
AAA	Authentication, Authorization, Accounting	MVNO	Mobile Virtual Network Operator
ABI	Application Binary Interface	NBAP	Node B Application Part
ADSL	Asymmetric Digital Subscriber Line	NTP	Network timing protocol
AMR	Adaptive Multi-Rate	OAM	Operations & Maintenance
API	Application Programming Interface	PHY	Physical layer
ARPU	Average Revenue Per User	PSTN	Public Switched Telephone Network
BSC	Basestation Controller	QoS	Quality of Service
DDR	Dual Data Rate	RAN	Radio Access Network
DECT	Digital Enhanced Cordless Telephone	RFIC	RF Integrated Circuit
DHCP	Dynamic Host Configuration Protocol	RLC	Radio Link Control (3G protocol)
DSP	Digital Signal Processor	RNC	Radio Network Controller
EV-DO	Evolution-Data Optimized	RRC	Radio Resource Control (3G protocol)
FMC	Fixed-Mobile Convergence	SCTP	Stream Control Transmission Protocol
FTP	File Transfer Protocol	SeGW	Secure Gateway
GPS	Global Positioning System	SIM	Subscriber Identity Module
GSM	Global System for Mobile communications	SIP	Session Initiated Protocol
H(e)MS	Home eNodeB Management System	SMC	Secure Monitor Call
HFA	Hardware Functional Accelerator	SNMP	Simple Network Management Protocol
HNB	Home Node B	TCP	Transmission Control Protocol
H(e)NB	Home evolved Node B	TCXO	Temperature controlled crystal oscillator
HSDPA	High-Speed Downlink Packet Access	UDP	User Datagram Protocol
HSS	Home Subscriber Server	UE	User Equipment
HSUPA	High-Speed Uplink Packet Access	UMA	Unlicensed Mobile Access
IMS	IP Multimedia Subsystem	UMAN	UMA access Network
IP	Internet Protocol	UNC	UMA Network Controller
IPsec	IP security (protocol)	VCTCXO	Voltage Controlled, Temperature Compensated Crystal Oscillator
LGW	Local Gateway	VoIP	Voice over Internet Protocol
ISP	Internet Service Provider	W-CDMA	Wideband Code Division Multiple Access
LTE	Long term evolution	WiFi	IEEE 802.11 wireless technology
Iub	Interface between 3G basestation & RNC	WiMAX	IEEE 802.16 wireless technology
MAC	Media Access Control (protocol layer)		