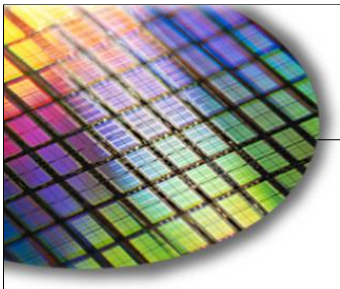


The World Leader in High Performance Signal Processing Solutions

Lockbox™ Secure Technology
on Blackfin® Processors

Presented by:

Phil Giordano
Senior Applications Engineer

About This Module

This presentation will familiarize the reader with the features, benefits, and high level operation of Lockbox secure technology on Blackfin processors.

Prerequisites: Familiarity with security and cryptography concepts.
Experience with embedded processors or systems.

Module Outline

1. **Introduction**
   - Defining Security Needs/Requirements
   - Lockbox Secure Technology on Blackfin processors
2. **Security Features on Blackfin**
3. **One-Time-Programmable (OTP) Memory**
4. **Authentication Process on Blackfin**
5. **Debug and Test Features**
6. **Summary and Conclusion**
7. **Resources and References**
8. **Glossary**
9. **Acronyms**

See ‘Resources and References’ for links and references which describe cryptographic concepts cited throughout this presentation.

See Glossary for more details of terms used throughout this presentation.

Defining Security Needs/Requirements

- **What are you trying to protect (i.e., code? data?)?**
- **What/Whom are you trying to protect it against?**
  - Who are typical adversaries (i.e., registered end users? hackers? competition?)?
  - What are the resources available to them? (i.e., typical consumer? well-funded organization? foreign government?)?
  - Is the threat rooted in content theft or reverse engineering fears?

Lockbox Secure Technology on Blackfin Processors

- **Lockbox secure technology incorporates a secure hardware platform for *confidentiality* and *integrity* protection of secure code and data with *authenticity* maintained by secure software.**
- **This secure platform provides**
  - A secure execution mode
  - On-chip secure ROM
  - Secure storage for on-chip keys
  - Secure RAM
- **Access to code and data in secure domain is monitored by the hardware, and any unauthorized access to secure domain is prevented.**
- **The secure ROM code establishes the *root of trust* for the secure software in the system.**
- **The secure RAM provides *integrity* protection and *confidentiality* for authenticated code and data.**
- **User-defined cipher key(s) and ID(s) can be securely stored in the on-chip OTP memory.**
- **Every processor ships from the Analog Devices factory with a Unique Chip ID value stored in the publicly accessible OTP memory area.**

OTP = One-time-programmable memory – non-volatile on-chip memory

See Glossary for more details of terms used throughout this presentation.

Lockbox Secure Technology Benefits

Authenticity/Origin verification

Lockbox secure technology allows for verification of a code image against its embedded digital signature, and provides for a process to identify entities and data origins.

Integrity

Developers can use a digital signature authentication process to ensure that the message or the content of the storage media has not been altered in any way. Integrity can be verified using Lockbox's authentication of digital signatures.

Confidentiality

Cryptographic encryption/decryption supports situations that require the ability to prevent unauthorized users from seeing and using designated files and streams. Lockbox's secure processing environment (Secure Mode) and secure memory support confidentiality.

Lockbox Secure Technology Benefits (continued)

- **Renewability**
  - Renewability refers to the updating of system components to enhance security.
  - Lockbox's Unique Chip ID enables end users to identify each Blackfin processor and hence each OEM device in which the processor resides.
  - This Lockbox feature can be used in support of revocation and renewability of licenses in case of security violations in digital rights management systems, for example:
    - Unique Chip ID, in combination with a trusted DRM agent (sourced by the OEM), enables developers to implement renewability in DRM systems.
    - Unique Chip ID provides capability to identify each OEM device and "blacklist" devices to remove them from a system.
  - Unique Chip ID can also be utilized to "bind" processor to one specific boot source/device. Facilitates antitheft schemes and prevents OEM device cloning.

Security Features on Blackfin

Blackfin Enhancements for Security—New Hardware Features

- **One-time-programmable memory (64k x 1 bit)**
  - Public OTP memory (4 kBytes)
    - Used to keep a trusted public key for proper authentication
  - Private (secret) OTP memory (4 kBytes)
    - Used to keep secrets only accessible in Secure Mode (example: secret keys for a cipher)
  - Unique Chip ID (stored in public OTP memory)
    - Can be used to prevent cloning of products (bind software—in a flash memory—to a single processor)
- **Secure ROM**
  - Used to store the authentication software (secure entry service routine, crypto)
- **Secure state machine**
  - Open Mode (unsecured)
    - Default power-up mode of the processor
  - Secure Entry Mode
    - Ensures integrity of authentication process
  - Secure Mode
    - Secure environment to execute sensitive code and protect data in on-chip memory
- **Hardware monitor**
  - Firmware execution is monitored for unexpected branches
- **System switches (SECURE_SYSSWT)**
  - Controls secure environment and prevents attacks using JTAG emulation, reset pin, or DMA memory accesses

Note: Open Mode = Unsecured Mode

-The private OTP is not required for the authentication. Typically, this private OTP can be used for storage of Symmetric Keys used for an encryption/decryption algorithm or cipher, to store some secrets, etc.

-The Unique Chip ID can be used to prevent cloning. For example, each OEM device may have a BF54x and a flash memory where the SW is stored. The Unique Chip ID contained in the public OTP of the BF54x will be copied to the flash memory by the manufacturer. The software can check that both numbers match before executing. Since each BF54x has a Unique Chip ID value, the software will not work if a hacker clones the flash memories. Each flash can essentially be “bound” to a single BF54x processor.

Software Components

On-chip ROM firmware for Digital Signature Authentication using:

SHA-1 and Elliptic Curve Cryptography (ECC)

RAM-based Security framework

Security Scheme

- **Security scheme is based upon the concept of authentication of digital signatures using standards-based algorithms and provides a secure processing environment in which to execute code and protect assets.**
- **Security features are completely optional.**
  - Developers can optionally use security features by programming an ECC public key into a specified area within public OTP memory and optionally program “secret” key(s) or other “secret” information in private/secret area of OTP.
  - Developers can choose not to use security features at all since Blackfin boots up in Open Mode (unsecured) by default and does not rely on any security features for normal operation in Open Mode—operates just like earlier Blackfins without Lockbox secure technology.
- **Public ECC key must be programmed into specified area within public OTP memory by developers in order to perform authentication and transition secure state machine through state flow.**

Standards-Based Algorithms

- **Lockbox secure technology uses standards-based cryptographic algorithms.**
  - Digital signature authentication on BF54x and BF52x utilizes the following:
    - Elliptic Curve Cryptography (ECC) asymmetric cipher[1]
      - The implementation of ECC is based on a binary field size of 163 bits.
    - SHA-1 secure one-way hash.[2]
      - SHA-1 produces a 160-bit (20-byte) message digest.
- **ECDSA signature verification, a subset of ECDSA, is implemented in the Blackfin BF54x and BF52x processors.[3]**
- **Open, published, trusted encryption algorithms and protocols are always better than a proprietary encryption algorithm and protocol.**
- **Preferred algorithms have been in the open literature for years and have withstood serious attempts to withstand shortcut attacks.**

[1] These implementations are based on the Elliptic Curve Digital Signature Algorithm (ECDSA) specified in FIPS 186-2 with Change Notice 1 dated October 5, 2001, Digital Signature Standard (DSS) (http://csrc.nist.gov/cryptval/dss.htm), and specified in ANSI X9.62-1998.

[2] SHA-1 is based on the publicly available standard for FIPS 180-2 (Secure Hash Signature Standard [SHS]) (FIPS PUB 180-2), http://csrc.nist.gov/CryptoToolkit/tkhash.html).

[3] ECDSA also includes other elements that these Blackfin products do not support, such as: Elliptic Curve Domain Parameter Generation and Validation; Key Generation and Validation; Signature Generation.

Open, published, trusted encryption algorithms and protocols are always better than proprietary encryption algorithms and protocols.

Preferred algorithms have been in the open literature for years and have withstood serious attempts to withstand shortcut attacks.

The processes used for digital signatures have undergone thorough technological peer review for over a decade. Digital signatures have been accepted in several national and international standards developed in cooperation with and accepted by many corporations, banks, and government agencies. The likelihood of malfunction or a security problem in a digital signature cryptosystem designed and implemented as prescribed in the industry standards is extremely remote, and is far less than the risk of undetected forgery or alteration on paper or of using other less secure electronic signature techniques.

Secure State Machine—Modes of Operation

- **Open Mode (unsecured)**
  - Default mode of processor upon power-up/reset/boot.
  - All secured system switches are deactivated.
  - OTP memory secrets are protected from access.
  - The chip is open; all features are available with no restrictions.
- **Secure Entry Mode (authentication)**
  - Firmware is executing out of internal memory to authenticate a loaded code image.
  - All secured system switches are activated.
- **Secure Mode**
  - Once authentication process results in success, device is in Secure Mode.
  - Mode of operation to perform sensitive decryption or execution of code.
  - OTP memory secrets are accessible.
  - Secured system switches are accessible to user (authenticated) code.

Secure System Switches (SECURE_SYSSWT)

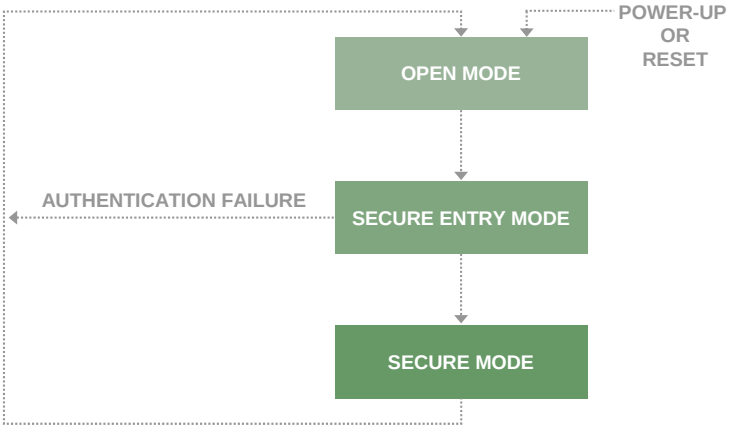
- **Secure system switches control hardware that could otherwise allow a threat of attack to a secured system.**
- **Software-controlled hardware protection mechanisms in Secure Mode and Secure Entry Mode.**
- **Disable all avenues of attack in support of a secured environment.**
- **Protect L1 instruction memory, L1 data memory, and on-chip L2 memory against unauthorized DMA accesses.**
- **Disable Analog Devices JTAG emulation instructions.**

During Open Mode the switches are involuntarily set with all controls off (unrestricted access) with exception of access to OTP protected private areas. OTP secrets are always protected and can only be accessible upon entry into Secure Mode.

During Secure Entry all switches are initially set with all controls on (restricted access). Access to the private OTP area remains restricted.

During Secure Mode operation all switches are voluntary (initially set) and under the control of authenticated code. Restricted access controls can therefore be reconfigured by authenticated user code.

Secure State Machine



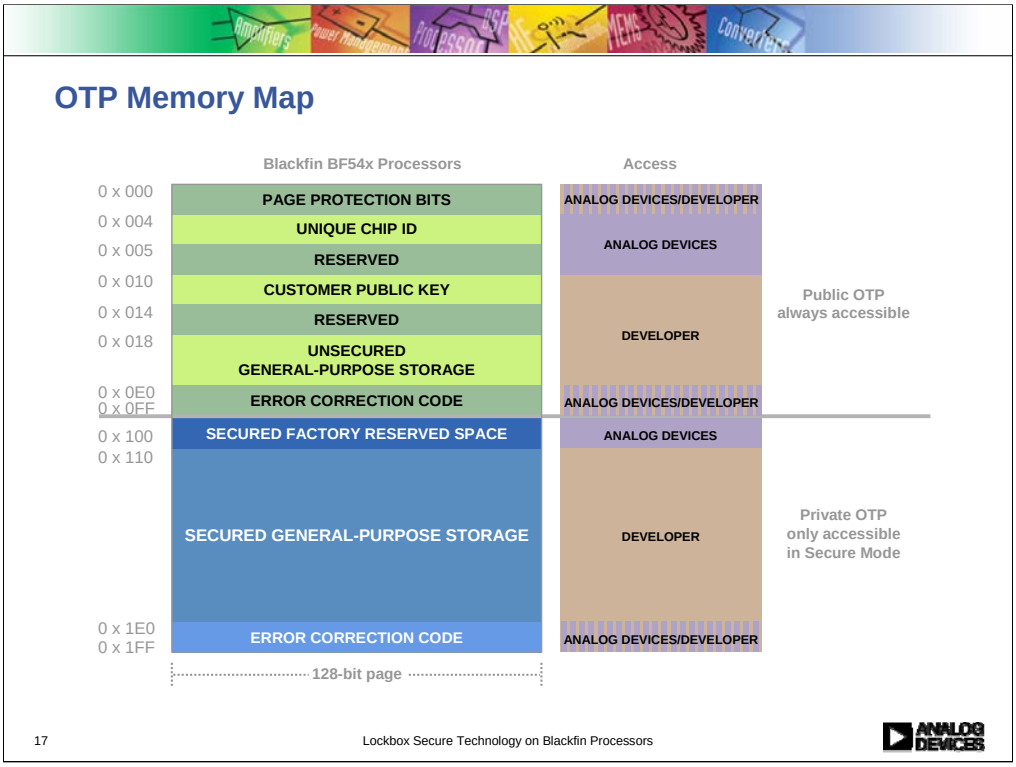
One-Time-Programmable (OTP) Memory

One-Time-Programmable (OTP) Memory

- **Serial one-time-programmable array (64k x 1 bits).[1]**
- **Public and private area access depends on hardware mode.**
  - Public area accessible in all modes (nonsecure).
    - Storage for nonsecure information such as public-key cipher keys, developer ID, product ID, Unique Chip ID, etc.
  - Private area accessible only in Secure Mode.
    - Storage for private keys for decryption of data or other validation.
- **Developer programmable and read accessible via normal code execution.**
- **Programming protection to guard against future tampering.**
  - Write protection scheme.
  - Limited access based on a Secure Mode setting.

[1] 64k x 1 array size applies to Blackfin BF54x and BF52x processors.

64kx1 OTP memory array size applies to ADSP-BF54x and ADSP-BF52x processors



The OTP is not part of the Blackfin linear memory map.

OTP memory is not accessed directly using the Blackfin memory map; rather, it is accessed via four 32-bit wide peripheral registers (OTP_DATA0-3) which act as the OTP memory read/write buffer.

The buffer has four 1- bit read/write locations for a total of 16 bytes.

The OTP memory controller organizes the memory's bit access into 128-bit pages. There are 512 pages within the array.

Each page is initiated by setting a page address and initiating read or write commands.

OTP array is 1 bit wide and all accesses are serial accesses.

64kx1 OTP memory array size and organizational structure described here applies to ADSP-BF54x and ADSP-BF52x processors

One-Time-Programmable (OTP) Memory

- **4 kB of public OTP memory = 256 pages x 16 bytes**
- **4 kB of private OTP memory = 256 pages x 16 bytes**
- **OTP memory accesses utilize error correction to ensure data integrity.**
  - Hamming code: Single error correction, double error detection.
    - Each 64-bit page has 8-bit hamming ECC in the *error correction code* field of OTP memory.
    - OTP read/write functions using error correction provided by Analog Devices.
- **The *Unique Chip ID* is programmed on every processor before leaving the Analog Devices factory.**
- **The *customer key* page stores developer's ECC public key.**
  - The secure entry service routine requires the public key here.
- **Approximately 50,000 bits of OTP are available for developer use.**

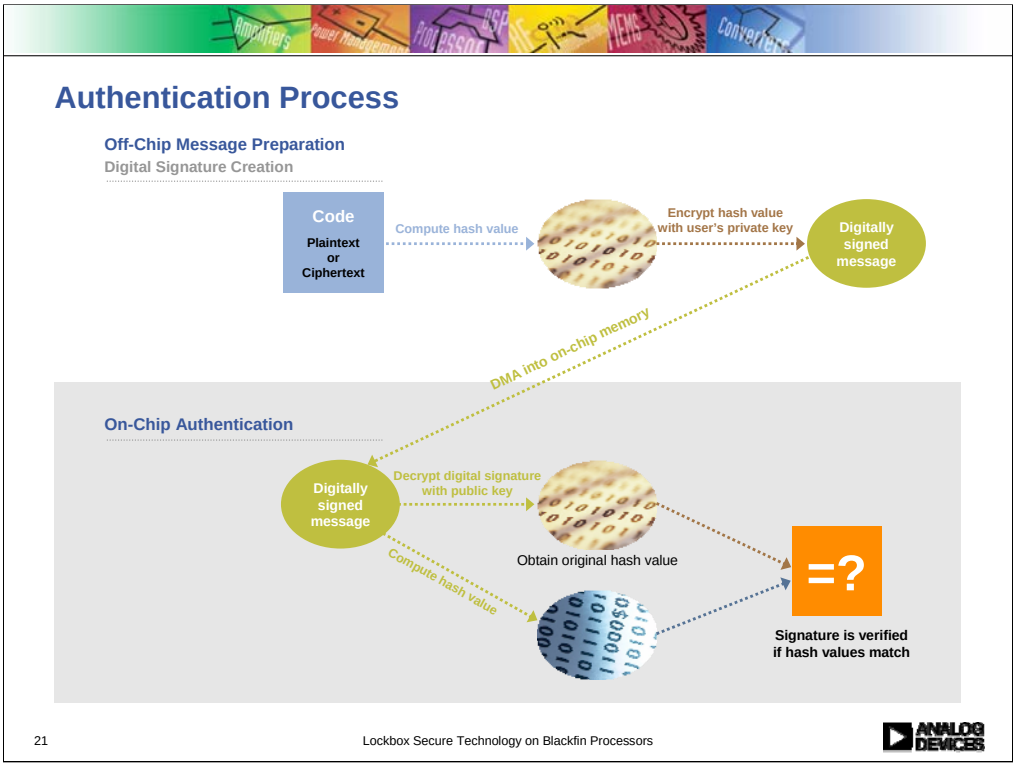
This information applies to Blackfin BF54x and BF52x processors.

OTP information on this slide applies to ADSP-BF54x and ADSP-BF52x processors

Firmware and On-chip ROM

- **Security is managed by firmware stored in on-chip ROM.**
  - Hardware extensions help to protect secrets.
  - Supports digital signature authentication and secure state machine flow through open (nonsecure), Secure Entry, and Secure Mode states.
  - Blackfin BF54x processors
    - 64 kByte L1 instruction ROM operates in the CCLK domain at CCLK frequency.
  - Blackfin BF52x processors
    - 32 kByte on-chip boot ROM operates in the SCLK domain at SCLK frequency.
- **On-chip ROM ensures *integrity* for security firmware.**
  - Code residing in ROM is tamper proof.

Authentication Process on Blackfin



Digital signatures are created using a public-key signature algorithm such as the ECC public-key cipher and a secure one way hash.

- A hash of the file is performed and the hash is signed instead of the file itself.
- SHA-1 is used to perform the hashing.
- ECC is used to encrypt/decrypt the hash result (cryptographic digest).

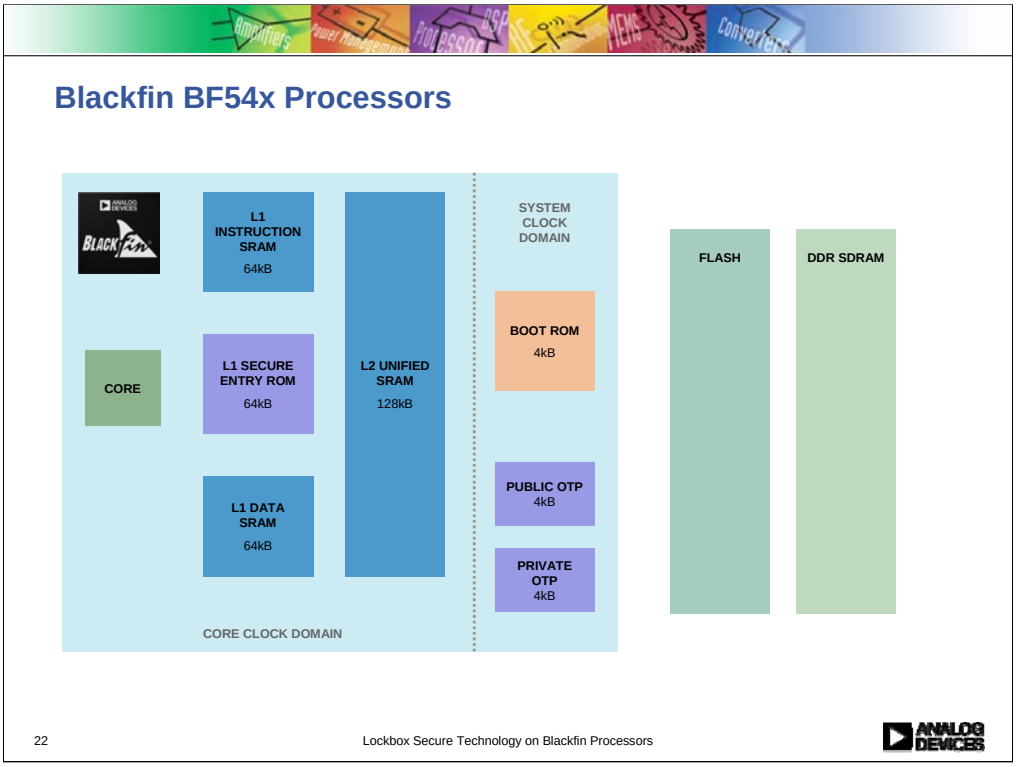
The following summarizes the Authentication process:

- Operations performed off-chip:
  - A one-way hash of the developer's application code is produced using SHA-1.
  - The hash is encrypted with the private key using ECC, thereby signing the file and creating a digital signature unique to the file.
  - The developer's digitally signed application code is DMA'd into Blackfin.
- Operations performed on-chip:
  - The Blackfin executes SHA-1 from firmware in on-chip ROM to produce a one-way hash of the file.
  - Using ECC, the Blackfin decrypts the signed hash with the user's public key stored in OTP.
  - Hashes are now compared.

If the original hash matches the hash calculated on the Blackfin, the signature is valid and the file is intact.

The developer's authenticated code is now allowed to execute in a secure manner in Blackfin internal memory.

Authentication failure results in a return to non-Secure Mode and the code attempting authentication is not allowed to execute on-chip with access to secrets in Secure Mode.



Basic block diagram of ADSP-BF54x family member.

Core. It will show where are we executing from at each of the steps (PC = program counter).

-L1 Instruction SRAM. Only code can be placed here. Runs at core clock frequency.

-L1 Secure Entry ROM. ROM that contains the security firmware. Runs at core clock frequency.

-L1 data SRAM. Only data can be placed here. Runs at core clock frequency.

-L2 unified SRAM. Code and data can be placed here. Operates in CCLK domain with some additional latency compared to L1 SRAM. See product manuals for details.

-Boot ROM. ROM that contains the boot kernel used to load an .ldr file into the corresponding memories. Runs at system clock frequency.

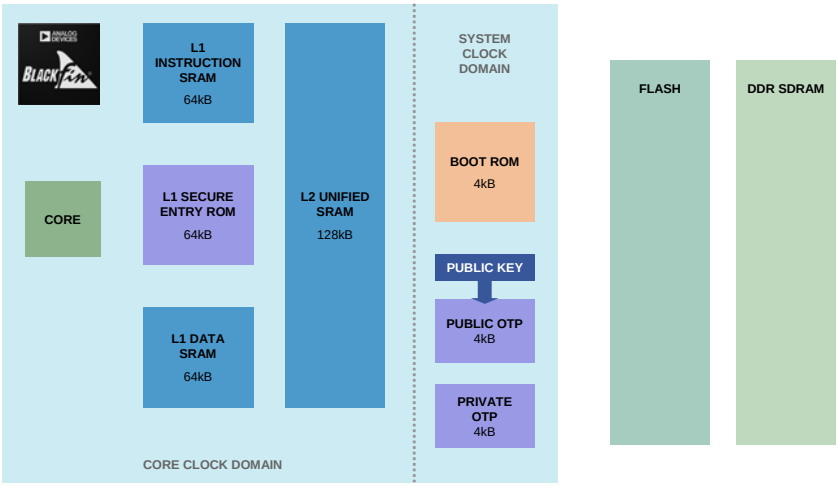
-Public OTP (one-time-programmable) and private OTP. Memory that can be written only once. It can be write-protected as well.

-The external Flash is shown for the examples. It is just a typical place where the application (code and data) is stored. Other interfaces/peripherals could store the application as well. The security scheme is not restricted to it.

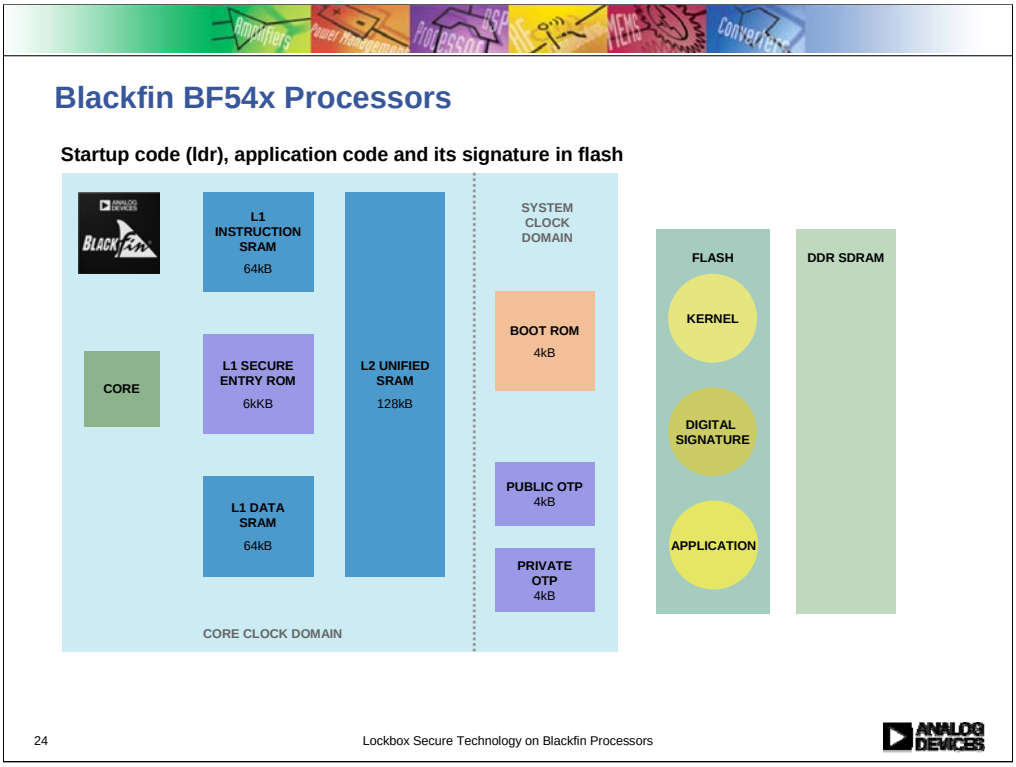
-The external DDR SDRAM is also a typical place where run-time data is stored. Only for example purposes. Other interfaces/peripherals could also be used. The security scheme is not restricted to it.

Blackfin BF54x Processors

Store the public key in public OTP memory



The public key is stored in the public OTP memory. OTP is programmable by developers and is typically programmed before releasing the product to end customers.



A small startup .ldr file created by the developer is stored in flash and is labeled as “kernel” in this example. This code is non-secure and is generated by the developer.

The secure application and its corresponding Digital Signature are stored in flash. The flash memory is our boot source in this example.

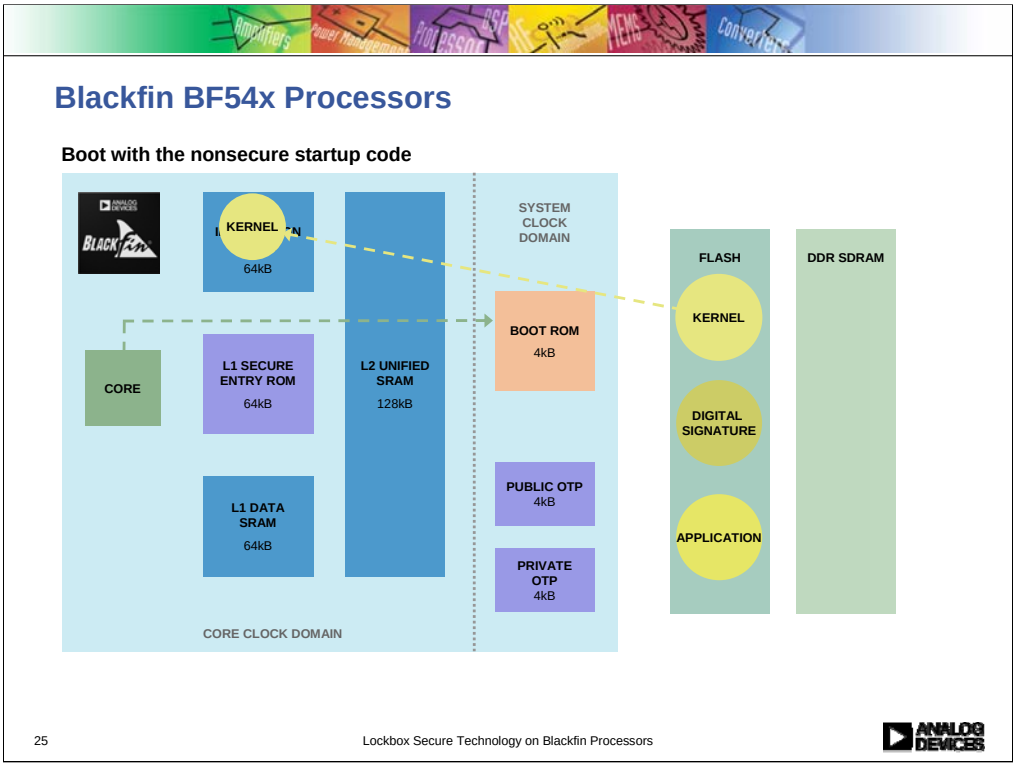
The *Digital Signature* is the encrypted Digest of the Application.

Notes:

-We are assuming for this example that we want to run a completely secure application. Therefore, it fits in internal memory.

-The BF54x and BF52x boot in an Open Mode. Therefore, a small non-secure startup code is required. This code will trigger the authentication process.

-There might be other customers/systems where most of the Application is non-secure and only a small routine is authenticated. This is also possible. The object labeled “kernel“ would actually be the non-secure Application and object labeled “Application“ would actually be the small routine to be authenticated.



Normal booting in Open Mode. The core executes the “boot kernel“ from Boot ROM

The Startup.ldr (kernel) is booted, the secure Application is ignored for now.

The Secure State Machine has 3 modes:

-Open Mode (Unsecured mode)

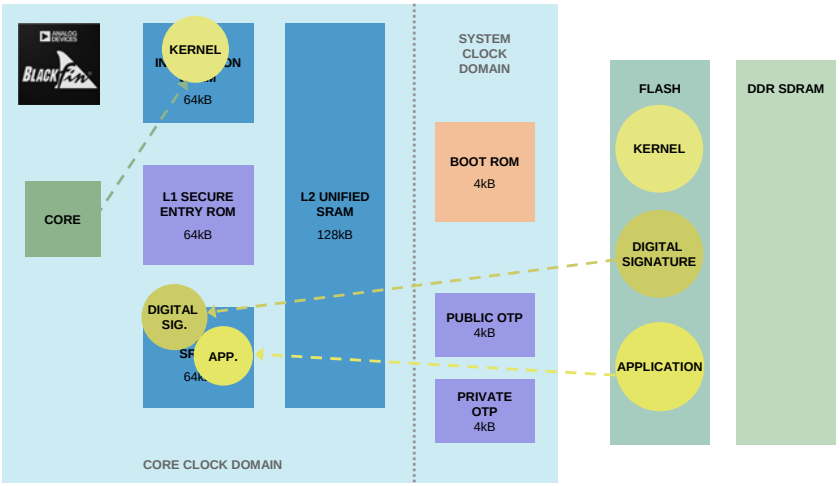
-Secure Entry Mode

-Secure Mode

Booting occurs in Open Mode

Blackfin BF54x Processors

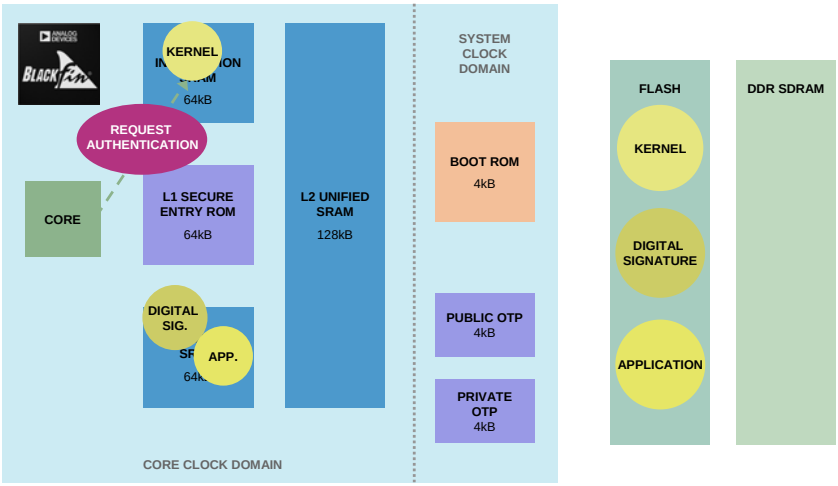
Load code/data and digital signature to internal memory



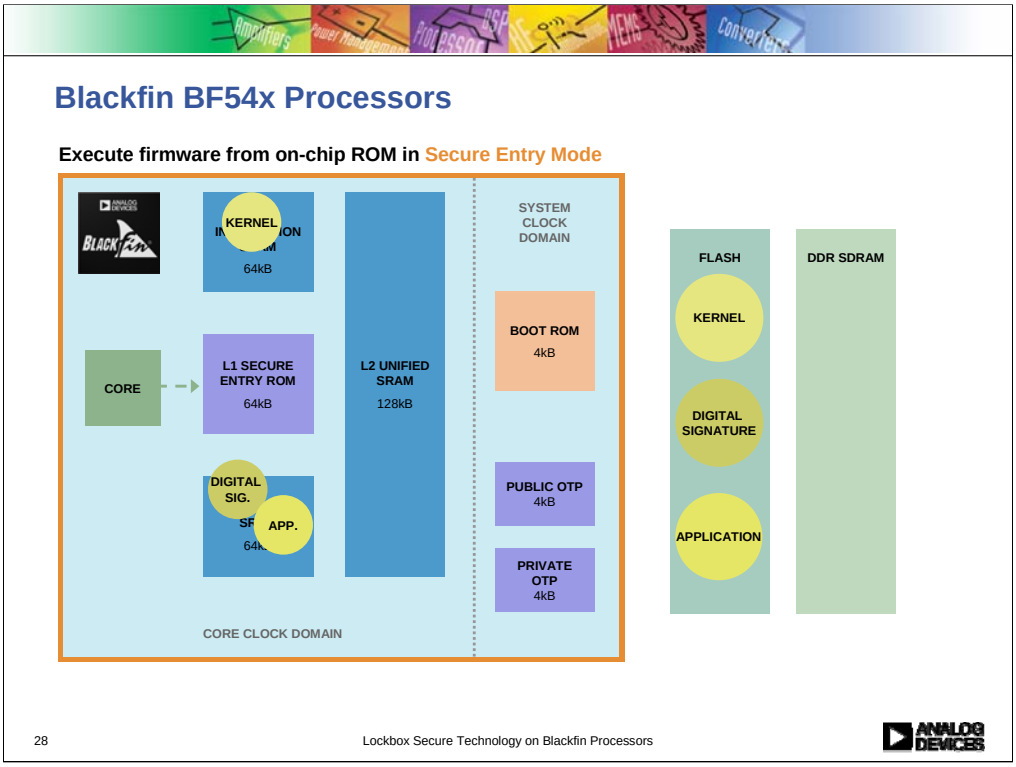
After booting, execute the startup kernel code. This code will prepare the Application to be authenticated.

Blackfin BF54x Processors

Request authentication and call the secure entry service routine



The non-secure kernel startup code requests authentication and calls the firmware Secure Entry Service Routine stored in on-chip ROM.



The Secure Entry Service Routine (SESR) starts the authentication process. The Core executes the SESR stored in on-chip ROM.

The Secure Entry Service Routine (SESR) is stored in on-chip ROM memory and controls the authentication process (also referred to as 'firmware').

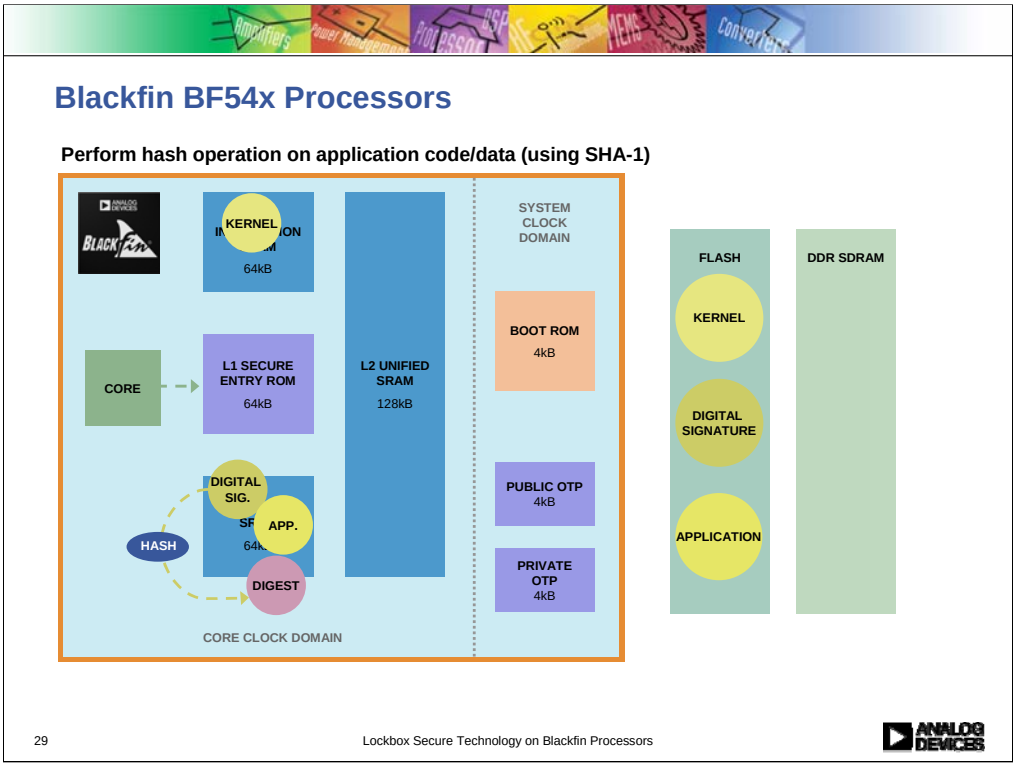
During Secure Entry Mode:

The Analog Devices private JTAG emulator interface is disabled (default).

DMA access to/from internal memory is disabled.

Safeguard mechanisms built in to the Blackfin hardware detect ANY deviation of the Program Counter outside of the address range encompassing the security firmware

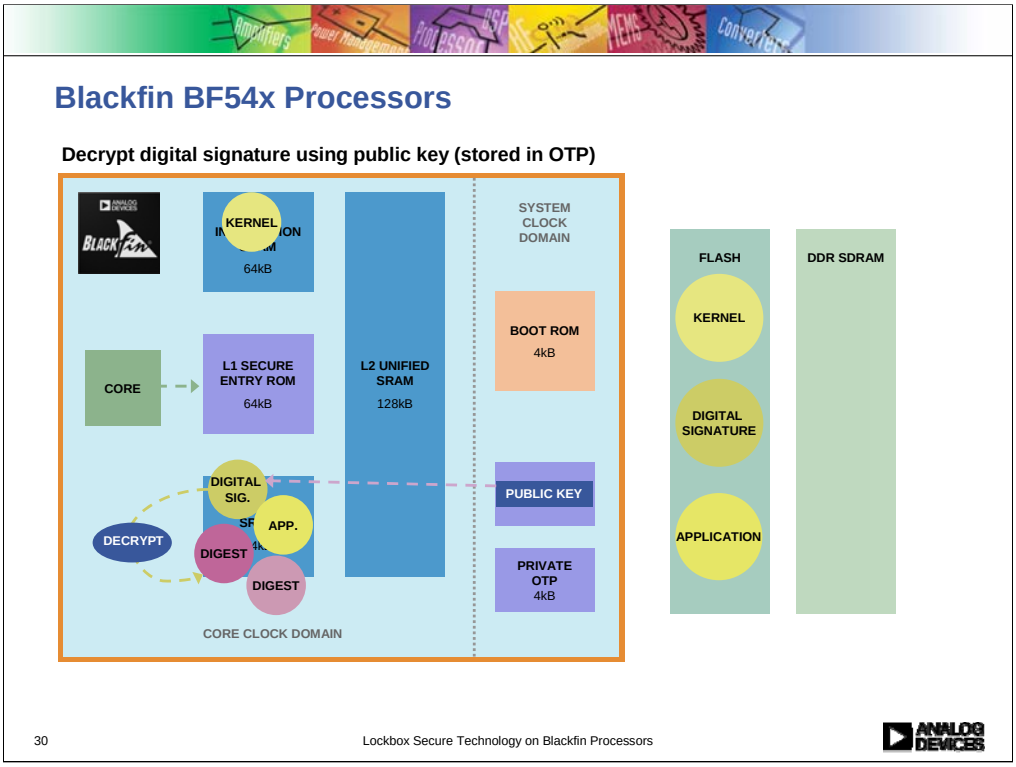
If the user enables interrupts and while executing SESR an interrupt is triggered, this interrupt will be serviced. However, vectoring outside of the SESR will be detected by the Blackfin hardware and the Secure State Machine will exit Secure Entry Mode and enter Open Mode. This results in failure of the Authentication process. The user's application can make another request for authentication to be repeated. Precedence can be given to the real time system events and is user-configurable.



Blackfin firmware performs authentication which consists of:

- Performing a hash operation on user's application code/data (using SHA-1).
- The encrypted digital signature is then decrypted (via ECC and public key stored in OTP on Blackfin).
- Compare original hash digest value with the result of the hash calculated on the user's application code within Blackfin on-chip memory.
- If they are identical, authentication results in success as this indicates that the user's application code/data has not been tampered with and can be trusted to execute on the Blackfin.
    - Decrypt the user's application code/data if it was encrypted outside the Blackfin prior to Boot/DMA. (For example, AES decryption uses a secret cipher key that can be stored in Blackfin private OTP memory area that is only accessible once authentication results in success and the processor is operating in Secure Mode). Decryption should be performed while operating in Secure Mode.

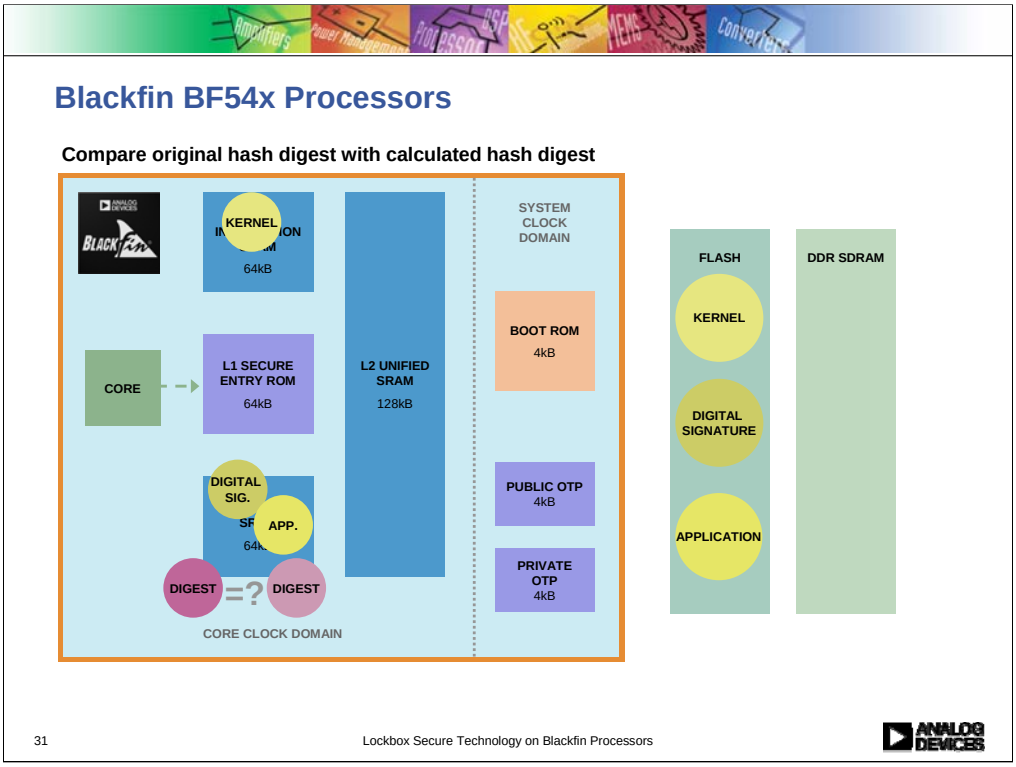
Execute the user's authenticated application code in Secure Mode on Blackfin.



The Digital Signature is decrypted using the Public Key from the trusted source stored in public OTP memory…

Note: To decrypt, the public key is used. The public key is stored in public one-time-programmable (***Public OTP***) memory. This one-time-programmable memory can be programmed by the developer and it can be locked (write protected) to prevent future alteration. By this means, BF54x and BF52x can help ensure that the public key stored in OTP is from the trusted source.

Elliptic Curve Cryptography (ECC) keys are used in Lockbox secure technology for Digital Signature authentication.

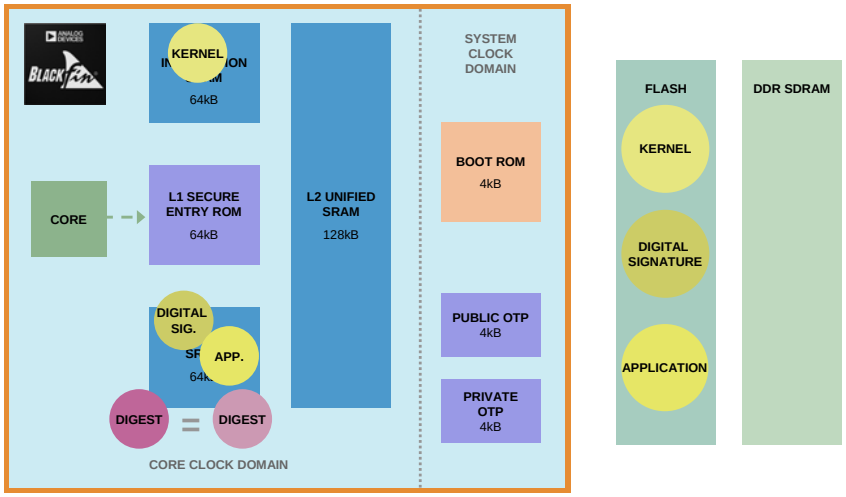


Compare the original hash digest with the hash digest calculated on-chip. If they match, the message is *Authentic*!

If both hash digest results match, the Secure State Machine enters ***Secure Mode***.

Blackfin BF54x Processors

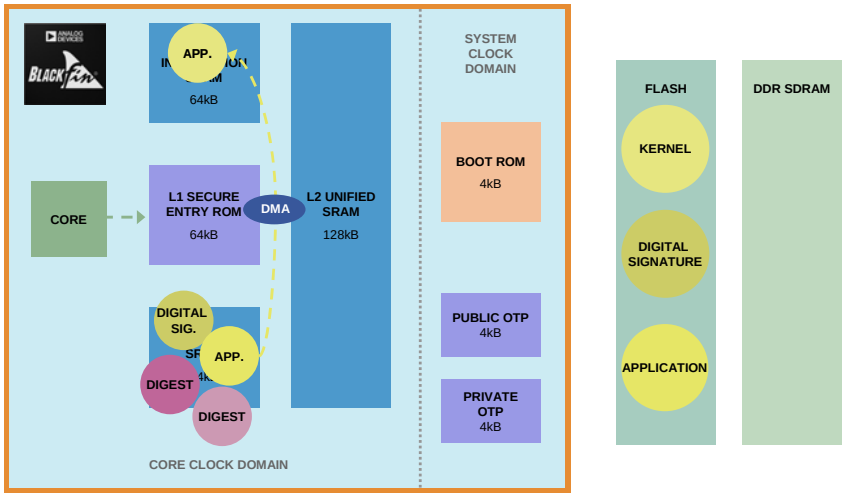
If hash digests match, authentication results in success



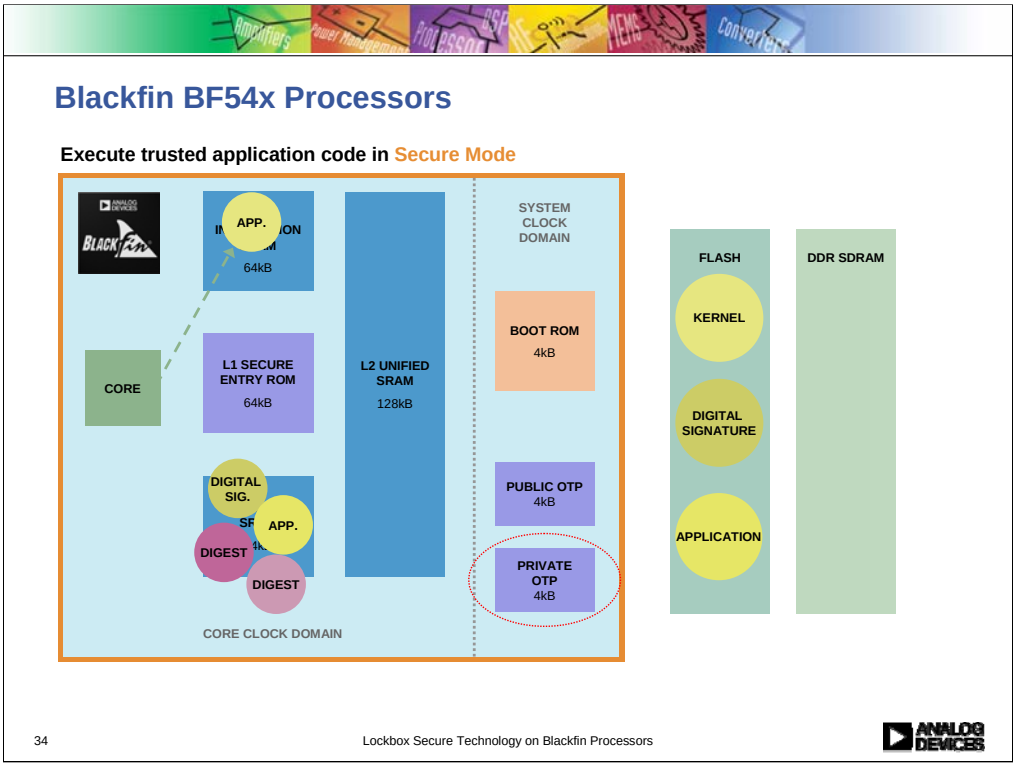
If both hash digest results match, authentication process results in success. Authenticated code will subsequently be allowed to execute on the Blackfin in Secure Mode.

Blackfin BF54x Processors

DMA the authenticated code to L1 instruction SRAM



Firmware automatically performs DMA transfer of authenticated code into L1 instruction memory (the user defines this with parameters passed to the SESR during request for authentication).



Authenticated (trusted) code is allowed to execute on Blackfin in Secure Mode.

Trusted code has control of Secure System Switches which control all access restrictions and protection mechanisms.

Private OTP memory area is now accessible to trusted code.

Debug and Test Features

Security and JTAG

- **Open Mode**
  - JTAG functionality is fully enabled and unrestricted.
- **Secure Entry Mode**
  - Analog Devices JTAG emulation is disabled (default, configurable in Secure Mode).
  - Firmware controls core execution, and JTAG emulation cannot be re-enabled.
- **Secure Mode**
  - Analog Devices JTAG emulation is disabled (default, configurable).
  - Analog Devices JTAG emulation can be enabled in Secure Mode.
    - The user must successfully go through the authentication process at least one time, and then program the secured system switches to enable emulation via execution of authenticated code.
    - Private JTAG emulation can be configured to be enabled for the current Secure Mode session only, or enabled in all modes of operation.
- **By default, Analog Devices JTAG emulation is disabled when the processor enters Secure Entry Mode or Secure Mode.**
- **Public JTAG instructions necessary for system test and debug (such as boundary scan and bypass mode) remain in effect and are not hindered by Secure Mode operation.**
  - Enables users to perform board level debug without interference from the Blackfin processor.

All supported public and private JTAG instructions remain operational when operating in Open Mode. All supported JTAG public features remain operational and all JTAG private features are disabled when operating in Secure Entry Mode and Secure Mode.

Analog Devices JTAG Emulation is part of the Private JTAG instructions.

Analog Devices emulators use the IEEE 1149.1 JTAG test access port of the processor to monitor and control the target board processor during emulation.

Summary and Conclusion

Flexible and Robust Security Scheme

- **Security scheme is based upon the concept of authentication of digital signatures using standards-based algorithms and provides a secure processing environment in which to execute code and protect assets.**
- **Mixture of hardware and software mechanisms combine to provide the following benefits for secure processing:**
  - Authenticity/Origin verification
  - Integrity
  - Confidentiality
  - Renewability
- **Security is optional.**
  - Developers can choose not to use security features at all.
    - Blackfin boots up in Open Mode (unsecured) by default.
    - Blackfin does not rely on any security features for normal operation in Open Mode.
      - By default, operates just like earlier Blackfins without Lockbox secure technology.
- **Platform for e-commerce, IP/code protection, and digital rights management support.**

Conclusion

- **Lockbox secure technology on Blackfin processors offers a flexible, programmable platform for securing code and data.**
  - Lockbox provides publicly accessible, user-programmable OTP memory that enables developers to program their own device IDs and helps to ensure that these device IDs remain tamper proof.
  - Lockbox features private, secure OTP memory that enables developers to program their own private device assets (for example: private keys) and to ensure that these assets are secure (not accessible, and invisible to unauthorized users) and tamper proof.
  - Lockbox's Secure Mode provides a secure processing environment in which only authorized code is allowed to access sensitive device assets.
    - This enables developers to implement systems in which only authenticated, trusted code can execute sensitive operations or gain access to confidential data.
  - Lockbox enables memory protection, thus providing secure storage and privileged access for confidential content.

Resources and References

Resources and References

- **Speaker notes are included on many slides within this presentation.**
- **Analog Devices website which has links to white papers, manuals, data sheets, FAQs, Knowledge Base, sample code, development tools and much more:**
  - www.analog.com/blackfin
- **For specific questions click on the "Ask a question" button.**
- **Additional URLs:**
  - http://www.rsa.com/rsalabs/
  - http://www.certicom.com/index.php
  - http://csrc.nist.gov/
  - http://www.cryptnet.net/fdp/crypto/crypto-dict.html
  - http://www.keylength.com/index.php
  - http://www.schneier.com/index.html

Textbook references:

- *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Second Edition, by Bruce Schneier, Wiley; 2 edition (October 19, 1995), ISBN: 0471128457.
- *Security Engineering: A Guide to Building Dependable Distributed Systems*, by Ross Anderson, Wiley (January 22, 2001), ISBN: 0471389226.
- *Handbook of Applied Cryptography*, by A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press, 1996. For further information, see www.cacr.math.uwaterloo.ca/hac.

Cryptography Made Easy

An Illustrated Guide to Cryptographic Hashes
http://www.unixwiz.net/techtips/iguide-crypto-hashes.html

Digital Signature GuidelinesTutorial
http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html

What Is a Digital Signature?
http://www.youdzone.com/signature.html

Cryptography Dictionary
http://www.cryptnet.net/fdp/crypto/crypto-dict.html

Wikipedia, the free encyclopedia
http://www.wikipedia.org/

(Search terms: cryptography, encryption, hash, Digital Signature, symmetric-key algorithm, public key cryptography)

Glossary

Asymmetric algorithm: A cryptographic algorithm that uses two different keys for encryption and decryption.

Authentication: Verifying a code image against its embedded digital signature. Process for identifying either entities or data origins.

Authentication control code: Firmware code stored in ROM to control secure state machine and hardware modes during the process of authentication.

Authenticity: The quality of actually having come from the source that is claimed.

Chip ID: Unique identification number per chip (stored in public OTP memory).

Ciphertext: Encrypted message.

Cleartext: Unencrypted message (synonymous with “plaintext”).

Confidentiality: Cryptographic means to ensure privacy or secrecy of information from unauthorized parties (so that only after authorized access, data can be read). Typically, confidentiality is ensured using data encryption via symmetric algorithms.

Digest: Secure digital fingerprint, created by a one-way hashing function.

Digital certificate: A piece of information digitally signed by a trusted third party, or certificate authority (CA), that establishes a user’s credentials and identity. Typically consists of developer’s public key and developer ID signed by a certification authority.

Digital signature: A digitally signed hash result of the message. Any digest encrypted with a developer’s private key.

Elliptic curve cryptography [ECC]: A class of cryptosystems that are based on the difficulty of finding points on an elliptic curve over a field with special properties. Most often, the strength of ECC is provided by the discrete logarithm problem; however, the factoring problem can also be used.

Integrity: Cryptographic means to ensure that the message or the content of the storage media has not been altered in any way. Integrity is verified using authentication.

References:

Cryptography Dictionary (http://www.cryptnet.net/fdp/crypto/crypto-dict.html)

Wikipedia (http://www.wikipedia.org/)

Glossary

Key management: Refers to the distribution, authentication, and handling of keys.

Nonrepudiation: Preventing an entity from denying previous commitments or actions.

Open Mode: Default operating mode of the processor in which nothing is restricted except for access to private OTP memory.

OTP: One-time-programmable memory. Customer-programmable via code executing on processor.

Plaintext: Unencrypted message.

Private key: Private (secret) part of asymmetric key used to create digital signatures.

Private OTP: Customer-programmable OTP memory area for private (secret) key and sensitive information storage. Accessible *only* in Secure Mode.

Public key: Public part of asymmetric key used to verify digital signatures.

Public OTP: Customer-programmable OTP memory area for public key and information storage. Accessible in all operating modes, including Open Mode, Secure Entry Mode, and Secure Mode.

Secret key: Any symmetric secret key (e.g., download key, key encryption key [KEK]).

Secure Entry Mode: Secure operating mode in which firmware controls the authentication process.

Secure Mode: Secure operating mode allowing execution of authenticated code, decryption of sensitive information, authenticated code access chip secrets in private OTP memory area, etc.

Secure RAM: Configurable part of internal system RAM accessible only in Secure Mode.

Security framework: Application code executed in RAM to pass parameters to authentication control code and invoke an authentication request.

Symmetric key algorithm: A cryptographic algorithm in which only one key is used to both encrypt and decrypt data.

References:

Cryptography Dictionary (http://www.cryptnet.net/fdp/crypto/crypto-dict.html).

Wikipedia (http://www.wikipedia.org/).

References:

Cryptography Dictionary (http://www.cryptnet.net/fdp/crypto/crypto-dict.html)

Wikipedia (http://www.wikipedia.org/)

Acronyms

AES: Advanced Encryption Standard specified in FIPS 197
ANSI: American National Standards Institute
CA: Certification Authority
DSA: Digital Signature Algorithm specified in FIPS 186-2
ECDSA: Elliptic Curve Digital Signature Algorithm
FIPS: Federal Information Processing Standard
HMAC: Keyed-Hash Message Authentication Code specified in FIPS 198
IV: Initialization Vector
MAC: Message Authentication Code
NIST: National Institute of Standards and Technology
PKI: Public Key Infrastructure
PRNG: Pseudorandom Number Generator
RNG: Random Number Generator
TDES: Triple Data Encryption Standard; Triple DES