AFRL-RY-WP-TR-2022-0195

ENABLEMENT OF GROUNDBREAKING SECURITY FEATURES IN INTEL STRATIX 10 FIELD PROGRAMMABLE GATE ARRAY (FPGA)

Richard Cliff, Tina Zhang, and Alexandra Schmidt

Intel Federal LLC

APRIL 2023
Final Report

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

See additional restrictions described on inside pages

© 2022 Intel Corporation.

STINFO COPY

AIR FORCE RESEARCH LABORATORY
SENSORS DIRECTORATE
WRIGHT-PATTERSON AIR FORCE BASE, OH 45433-7320
AIR FORCE MATERIEL COMMAND
UNITED STATES AIR FORCE

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the Air Force Research Laboratory (AFRL) Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RY-WP-TR-2022-0195 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH THE ASSIGNED DISTRIBUTION STATEMENT.

//signature//

JONATHAN I NICHOLSON, USAF 1st Lt
Program Manager
Trusted Electronics Branch

//signature//

SKYLER R. HILBURN, USAF Maj, Chief
Trusted Electronics Branch
Subsystems Technology Division

//signature//

GENE M. WILKINS, Lt Col, USAF
Deputy Chief, Aerospace Components &
Subsystems Technology Division
Sensors Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

*Disseminated copies will show "//signature//" stamped or typed above the signature blocks.

REPORT DOCUMENTATION PAGE

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED	
		START DATE	END DATE
April 2023	Final	25 June 2019	31 March 2022

4. TITLE AND SUBTITLE

ENABLEMENT OF GROUNDBREAKING SECURITY FEATURES IN INTEL STRATIX 10 FIELD PROGRAMMABLE GATE ARRAY (FPGA)

5a. CONTRACT NUMBER	5b. GRANT NUMBER	5c. PROGRAM ELEMENT NUMBER
FA8650-19-C-1742	N/A	N/A
5d. PROJECT NUMBER	**5e. TASK NUMBER**	**5f. WORK UNIT NUMBER**
N/A	N/A	Y1ZG

6. AUTHOR(S)

Richard Cliff, Tina Zhang, and Alexandra Schmidt

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Intel Federal LLC
4100 Monument Corner Dr.
Fairfax, VA 22030

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)	11. SPONSOR/MONITOR'SREPORT NUMBER(S)
Air Force Research Laboratory, Sensors Directorate Wright-Patterson Air Force Base, OH 45433-7320 Air Force Materiel Command, United States Air Forces	AFRL/RYD	AFRL-RY-WP-TR-2022-0195

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

PAO case number AFRL-2023-1487, Clearance Date 30 March 2023. © 2022, Intel Corporation. This work was funded in whole or in part by Department of the Air Force contract FA8650-19-C-1742. The U.S. Government has for itself and others acting on its behalf an unlimited, paid-up, nonexclusive, irrevocable worldwide license to use, modify, reproduce, release, perform, display, or disclose the work by or on behalf of the U. S. Government. Report contains color.

14. ABSTRACT

To accelerate the security features that enable Root of Trust and security requirements for the Freedom Creek MCP program, Intel's Programmable Solutions Group leveraged the Stratix 10 FPGA, with its processor-based Security Device Manager (SDM) and sectorized configuration scheme, to provide a wide range of new security capabilities. The commercially developed security features are available for use on the Stratix 10 FPGA for use in any new commercial or military system requiring improved trust and robust security capabilities. Using the Stratix 10 FPGA as a platform, Intel developed security features that do not require specific militarily critical technical data - (1) Physically Unclonable Function (PUF) based key cryptography, (2) Trust Platform Module capabilities, (3) SDM based anti-tamper capabilities, and (4) Secure platform attestation."

15. SUBJECT TERMS

FPGA Security feature Acceleration

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT	b. ABSTRACT	C. THIS PAGE		
Unclassified	Unclassified	Unclassified	SAR	24

19a. NAME OF RESPONSIBLE PERSON	19b. PHONE NUMBER *(Include area code)*
Glen Via	N/A

Table of Contents

Section **Page**

Approved for public release. Distribution is unlimited.

List of Figures

Figure **Page**

Approved for public release. Distribution is unlimited.

List of Tables

Table **Page**

Approved for public release. Distribution is unlimited.

1 SUMMARY

The AFRL – Intel Federal LLC contract FA6850-19-C-1742, was successfully commenced starting technical execution on July 1, 2019. A successful face to face technical interchange kickoff meeting was held with the AFRL program manager and representatives of other government agencies in Santa Clara, California. Expectations were set on contract deliverables and a high-level schedule presented. Intel presented a more detailed view of the four work packages.

Since then, Intel has completed development of the four work packages as originally defined on Stratix 10 with one modification of retargeting the Crypto services feature (sometimes referred to as Trust Platform Module or TPM) to Agilex. As the program was completed with some funds remaining, additional tasks were added with the AFRL program manager's agreement to migrate the remaining features to Intel's latest FPGA family – Agilex. At completion of the contract all four features are available on Agilex and all but crypto services are available on Stratix 10.

All of the features have been developed to a production level quality using Intel's Secure Design Lifecyle development process and released in Intel's Quartus Prime development FPGA development toolset. This report uses a Quartus release terminology to denote when the features became available. A Quartus release of 21.4 would denote that the feature was released at the END of the fourth quarter of 2021 for example.

The Intel PSG customer services group has, in parallel under Intel funding, developed a set of application notes and user guides to assist developers in using the new security capabilities.

Meetings between Intel and AFRL have been held monthly, with a technical deep dive into one of the features each quarter. Quarterly reports have been published describing development progress and highlighting next steps for the following quarter. Demonstrations have been successfully completed for each of the work packages.

Approved for public release. Distribution is unlimited.

2 INTRODUCTION

Stratix® 10 and Agilex are Intel's recent generation high end FPGA families with Agilex being introduced into the market in 2020. They were both developed by Intel's Programmable Solutions group (PSG), formerly Altera Corp.

Stratix® 10 and Agilex support state of the art programmable technologies with up to 5.5M logic elements, substantially faster performance and lower power, with up to 10 TFlops of compute power. Built on Intel's 14nm technology it employs a 3D integration strategy, with all of the high speed serial interfaces implemented on separate "chiplets" and integrated in-package using Intel's EMIB technology providing a wide range of product variants to be tailored to different application requirements.

Stratix® 10 can also support a wide range of ground-breaking security features targeted for any new commercial or military system requiring improved trust and robust security capabilities. This is achieved through a revolutionary processor-based configuration and security system containing the three innovations:

1) Security Device Manager (SDM)
2) Sectorized FPGA core
3) Bus based communication system to enable independent access to the sectors.

The new configuration and security features are now created through updateable firmware that runs on the processor based SDM (instead of the prior fixed state machine-based architecture), enabling new security capabilities to be added over time and existing ones to be improved. Accordingly, Stratix® 10 security can adapt to emerging requirements and attack threat vectors.

As the configuration system is now processor based, all configuration and security capabilities are created by developing firmware. Although Stratix® 10 has been shipping in production since the end of 2017, to date only the firmware for legacy features has been developed.

The AFRL funded project develops the above-mentioned firmware to cover the security features listed in Table 2-1 over the period of two years resulting in production quality security capabilities, years ahead of Intel's planned rollout.

One feature listed below (Trust Platform Module) will initially be released on the next generation FPGA Agilex®, with the remaining three features to be ported over by the end of the period of performance. Agilex® has the same cutting-edge benefits of the Stratix® 10 FPGA but with 45% higher performance and significantly more storage capacity.

Approved for public release. Distribution is unlimited.

Table 2-1: The four work packages that create the new Stratix 10 and Agilex features

Key Items	Value
Security Capability	**Description**
Physically Unclonable Function (PUF) based Key Cryptography	Secure key generation and management for encryption, authentication, attestation and user key provisioning
Trust Platform Module capabilities (Crypto as a Service)	Enable the FPGA's security IP for use in customers design
Anti-tamper capabilities	Detect and respond to wide range of attack vectors
Secure Boot and Measure Boot	Secure Boot and Measure Boot

Approved for public release. Distribution is unlimited.

3 METHODS, ASSUMPTIONS, AND PROCEDURES

Stratix 10® and Agilex® New Configuration and Security Hardware

Historically, FPGAs utilized a fixed state machine-based configuration scheme, where security features such as bitstream scrubbing and FPGA configuration encryption were embedded in hardware and added incrementally over time. Since the configuration system was state machine based, the past security solutions were “hardened” into the FPGA. With Intel’s Stratix 10 and beyond, Intel FPGAs have a revolutionary, processor-based programming scheme with all security and configuration functions located in the Secure Device Manager block (SDM). The SDM interfaces with the FPGA fabric core, partitioned into independent configuration sectors, through a bus-based configuration network. This provides a massively flexible configuration and security system controlled by configuration firmware that runs on the SDM processors (see Figure 2-1).

The SDM has a wide range of cryptographic hardware as shown in Figure 2-2 which, when combined with the flexibility of the FPGA, creates a platform to develop many advanced security capabilities and a sandbox to experiment with new capabilities to address emerging attack vectors. As these are developed by writing firmware to run on the SDM processors, they can be enhanced over time or upgraded via FPGA configuration updates to address new security threats as they emerge.

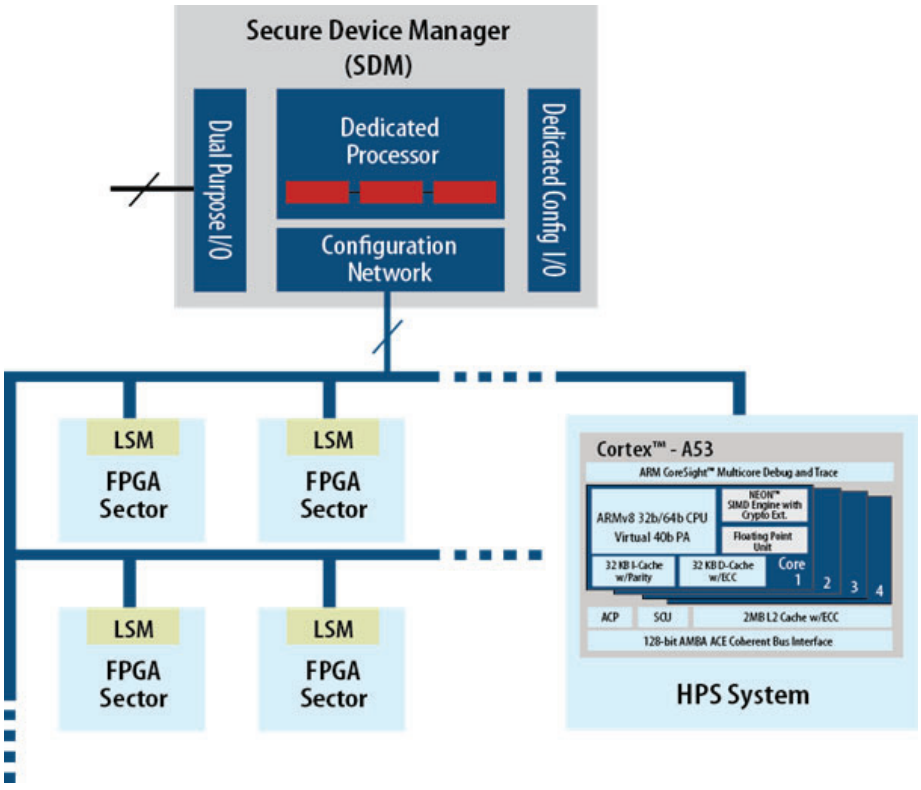

Figure 2-1: Secure Device Manager Controls Device Configuration and Security

Approved for public release. Distribution is unlimited.

Secure Device Manager Capabilities

The Secure Device Manager shown in Figure 2-2 has the following features:

1. Triple redundant processor for lockstep operation
2. Crypto IP (AES 256, SHA 256/384, ECDSA 256/384)
3. Tamper detection sensors
4. PUF source & key vault for creation and wrapping of keys
5. Bitstream compression and encryption/decryption
6. Access to the programmable logic core, controlled through a secure mailbox system.

On power up, the SDM firmware is authenticated with one or more digital signatures and then loaded into the SDM processors. Once complete, SDM performs all of the configuration and security functions during both the configuration and user operating mode. The SDM is controlled by a triple-mode redundant (TMR) processor synchronously clocked on a voting circuit, each with ECC to memory (cache). The TMR enables fault tolerant capabilities for all operations, ensuring error free behavior. The IP in the SDM has also been developed to be resistant to power attacks.

The core logic fabric is partitioned into separate, individually configurable “sectors”, with independent programming control, reprogramming, and monitoring of each sector, creating an unmatched regional control of the device.

Each sector has its own processor-based manager called the Local Sector Manager (LSM) that communicates with the SDM via a bus-based configuration network using a packet-based protocol. The LSM controls the programming and readback functions of the configuration memory within each sector.

User defined security solutions can also be created using the SDM’s ability to interface through a secure letterbox with user created “soft”, logic fabric-based IPs and programmed into the core logic fabric. Combining the programmability of the FPGA with the flexibility of processor-based security management enables a wide range of security possibilities. For example, different configuration memory scrubbing schemes can be deployed or advanced cryptographic algorithms can be used to encrypt or decrypt IPs or data within the users FPGA design. New security solutions can be tailored against emerging attack vectors.

Approved for public release. Distribution is unlimited.

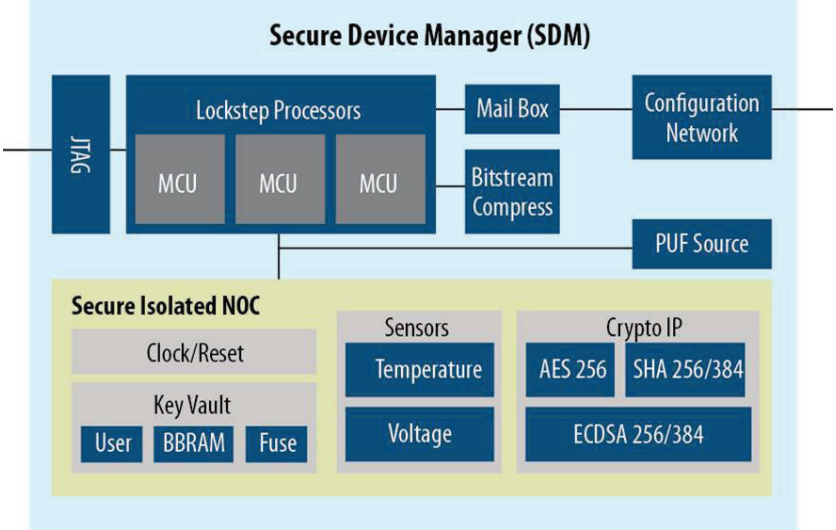

Figure 2-2: Secure Device Manager (SDM) Block Diagram

Because the SDM block controls the FPGA/SoC configuration process through firmware instructions, and can itself receive different firmware loads to manage this configuration (though always authenticated), this security scheme makes it possible for the Stratix® 10 and Agilex® products to have different configuration processes, orders, and encryption and authentication procedures.

The security features are enabled through the development of firmware that runs on the configuration processors. The firmware is loaded first into the FPGA and stored in internal SDM memory. The firmware programs the processors to utilize the function blocks in the SDM to create the desired security capability. For example, on power up the FPGA programming file can be first authenticated, decrypted and then decompressed using a combination of the PUF, key vault, AES256 and decryption blocks in the SDM.

New security features as defined in this proposal will be created by developing additional firmware to be added to the baseline configuration related firmware already developed.

This project's firmware development is done through Intel's Secure Design Lifetime (SDL) development process.

(a) Security feature specification finalization
(b) FPGA SDM firmware development
(c) System solution verification
(d) Security audit

The stages of the SDL process include exploration, planning, development, and production: these are shown in Figure 2-3 below.

Approved for public release. Distribution is unlimited.

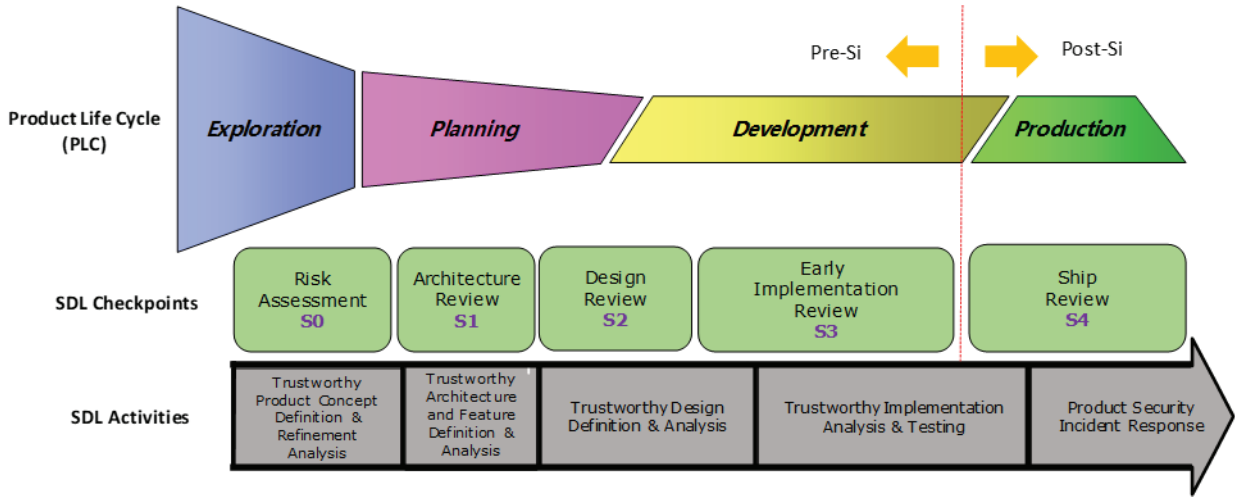

Figure 0-1: Secure Design Lifecycle

Approved for public release. Distribution is unlimited.

4 RESULTS AND DISCUSSION

4.1 Technical Staffing

Intel's leadership team that drove the technical direction of this program include:

Richard Cliff: Principal Investigator

Sridhar Rajagopal: Firmware Manager

Geoffrey Strongin: System Security Architect

4.1.1 Additional Staffing

Contracts Manager: Jannine Rhee

Program Manager: Alexandra Schmidt

Project Controls Analyst: Sameer Bandukda

Updates this Quarter

N/A – Program work has been completed

4.1.2 Subcontracts

This program has two subcontractors - University of Texas at Austin and Riscure – which were signed under contract in the first quarter of execution. The University of Texas at Austin is supporting work as it relates to PUF Enablement. Details on their performance can be found in the PUF enablement work package section. UTA work has completed with the final report submitted for review.

Work with Riscure started in Q1 of 2020 as planned with a kickoff meeting and a subsequent series of information gathering and planning meetings where the scope of their investigation has been outlined. Intel has provided two FPGA Development Kits for them to conduct work on behalf of this project. The final report has been delivered. Work with both subcontractors has been completed.

Funding for Intel Corp. employees is included in the Subcontracting Plan.

4.1.3 Property Procurements

Four FPGAs development boards were received. All boards have been shipped to AFRL.

4.1.4 Activity Summary

The Crypto Services feature was completed and released in the Quartus Prime 21.3 release.

The final demonstration was performed at a face-to-face with AFRL at Intel's Austin site. All four original work packages have been completed and released, with all planned features

Approved for public release. Distribution is unlimited.

successfully ported to Agilex where applicable. CAVP certification exploration was completed with a potential future path forward suggested. Significant progress was made on the development of the demonstration tool (aka Northcove) with the final release of the tool planned for Q3/Q4'22.

4.1.5 Budget

The program ultimately ran over budget, with Intel agreeing to fund all costs over the original AFRL budget.

4.1.6 Risks

N/A – Work on program is complete.

4.2 Work Package 1 - PUF Based Key Cryptography Enablement

4.2.1 Scope

This work package enables a Stratix® 10 and Agilex FPGA user to access the PUF embedded in the FPGA hardware through the device configuration process. The PUF is a device specific secret used for key protection, key material generation and device identification purposes. Specifically, the PUF generates a device-unique, unclonable key that designers can use for device authentication and key wrapping. PUF enablement will be successful when four subprojects including (1) Error control coding development, (2) Root Key generation, (3) AES Key Wrapping, and (4) Remote attestation key generation are completed.

4.2.2 Development Summary:

PUF Entropy Validation:

Professor Orshansky from University of Texas at Austin was subcontracted to provide analysis of the Intrinsic ID PUF integrated into Stratix 10. University of Texas initiated the process to work with Intrinsic ID (IID) so that they could get access to their algorithms for the Activation code generation. The end goal was to compare these algorithms with known error codes to determine if the IID algorithm and the Intel SRAM meets the bar with respect to key entropy.

University of Texas completed their study of the IID implementation. They decoded the encoding scheme used by IID and compared it with their theoretical analysis done earlier in the project. They were able to determine that the PUF helper data does not leak entropy based on the encoding and debiasing scheme used by the IID logic to generate the PUF helper data.

They were also able to calculate the probability of key re-construction failure on activation of PUF based on possible Bit Error Rates and SRAM biasing. When Intel's SRAM data was used for this analysis the reconstruction failure was less than 10^{-9}. The PUF analysis final report has been shared with AFRL.

For the PUF RAM characterization, the FW team worked with Intel Manufacturing on PUF RAM test for stability, bias, and bus access. Volume testing was performed on 8000+ units. In parallel, the FW team collaborated with the Intel Platform team on PUF RAM data collection for engineering devices for additional analysis with Intrinsic ID team and Professor Orshansky from University of Austin.

Firmware Development:

The firmware team implemented development flow to enable a user to use the PUF to wrap their AES root key. The code was verified and released initially as a beta in the 20.1 release of Quartus Prime and then updated to a production worthy version in 20.3. A demonstration to AFRL of the PUF operation was performed on 5/25/2020.

As part of the added activities to Glen Pass, porting of PUF firmware to Agilex was completed and released in Quartus Prime v21.4. This includes the user IID PUF (User performs their own enrollment in their OEM) and the UDS IID PUF (Intel manufacturing provides helper data) in security applications. Example applications are user AES key wrapping, platform attestation, crypto service keys protection etc.

Note that as the PUF hard IP integrated into both Stratix 10 and Agilex is from Intrinsic ID, it requires the acquisition of a license that can be obtained through Endosec. This is typical in the industry with PUF technology.

4.2.3 Scope

The SDM has embedded cryptographic functions it uses for its own purposes (bitstream encryption/decryption for example) can provide certain cryptographic services (AES256, SHA256/384 etc.) to the rest of the FPGA, saving significant soft logic resources in the case of the FPGA Encryption/Decryption services. This is done by providing commands to the SDM mailbox that then allows files of any size to be sent to the SDM via a streaming interface. Intel has developed Encryption/Decryption services, HMAC signing and verification, ECDSA signing and verification, and a user key management system. This capability is known today as Crypto Services although it has been called Trust Platform Module in earlier documentation and reports.

4.2.4 Development Summary

The Crypto Services work package was released in Quartus 21.3. The release is supported through both the FPGA fabric and the HPS. In other words, either the FPGA or the HPS embedded ARM embedded processor can send files to the SDM for encryption/decryption, hashing or other crypto functions. Soft IP logic was also developed to allow the crypto services to be connected to a user’s design in the FPGA fabric.

A recent improvement (Quartus 22.1) has now enabled the SDM to support hash functions of unlimited file size removing the previous size limit restriction of 500Mbytes.

Approved for public release. Distribution is unlimited.

One of the additional tasks added to this work package was a research project into current hardware and firmware limitations to certification. At the time of conception of the SDM hardware and the architecture development of the firmware, certification of the security solutions at that time was not commonly requested in the industry. This has recently become an important requirement.

Both the hardware and software has been analyzed for the SDM cryptography and the learning will be incorporated into future Intel FPGA products with a goal to ultimately support FIPS level 3 certifiability. Note, as certification ultimately covers the customers design as well as the FPGA hardware and firmware, the certification activity would take place on the end users system. Intel's objective is to prove that the SDM hardware and software is *certifiable* to enable the customer to achieve certification.

The crypto services feature was demonstrated in the AFRL face to face meeting held on March 31, 2022 at the close of the program.

4.2.5 Scope

The device can monitor voltage, temperature conditions, control registers status, aberrant clocking behaviors, as well as customer developed "soft canary circuits" (circuits developed by the customer to detect timing anomalies resulting from side channel attacks) for evidence of physical attack and can take measures such as zeroization of volatile encrypted keys and device configuration if desired. This shall be developed by enabling detecting sense functions, response functions, clean/zeroization functions, and firmware hardening.

4.2.6 Development Summary

The anti-tamper features for Glen Pass build upon some existing basic tamper resistance capabilities which included the ability to measure temperature and voltage and signal a potential attack event if either of these parameters exceeded thresholds. Glen Pass improved upon the measurement techniques and provided a wide range of tamper responses. There are different levels of response that can be set by the user; from simple reset and reconfiguration to a variety of scrubbing options including registers, memory bits. In the limit there is a kill device option that can be enabled. Clearly, this has to be done with great care as it is irreversible. A successful demonstration to AFRL of the Stratix 10 anti-tamper capabilities was completed on 10/28/2021. Detailed anti tamper functionality and modes of operation are documented in the user guides provided.

Anti-tamper firmware was successfully migrated to the Agilex family and incorporated into the Quartus Prime 21.4 release. The functionality in Agilex will be identical but will apply to a broader range of devices (VID).

Approved for public release. Distribution is unlimited.

4.2.7 Scope

The Stratix® 10 FPGA can perform the function of secure boot for a system, and for a processor, can manage the boot authentication across the whole system performing a Root of Trust capability across a system. In the case of measured boot, it provides accounting of the boot steps for correct operation. This shall be done in two steps: First configuration and Partial reconfiguration attestation.

4.2.8 Development Summary

The attestation verification activities were completed as planned and the feature for Stratix 10 was integrated into the upcoming Quartus 21.1 release. The initial release supported attestation through the FPGA. The HPS (embedded ARM processor) library components that enable HPS interoperability for attestation were delivered in a separate HPS release at the end of April 2021

Attestation was demonstrated successfully to AFRL in on 6/08/2021.

The attestation development work on Stratix 10 was significantly modified to be SPDM compatible as part of the Agilex migration as an Intel funded (non Glen Pass) activity.

An added component to this work package was the creation of a system level demonstration of the Attestation feature to create a Trusted Execution Enclave between a Xeon Processor and an FPGA is in progress. The plans and technical update for this activity were shared in the face-to-face meeting with AFRL on March 31, 2022. The project at this point is 80% done and will be completed using Intel funding. It is on schedule to be ready for demonstration in Q3 2022.

Approved for public release. Distribution is unlimited.

5 CONCLUSIONS

Intel has completed all items of the four work packages originally planned for this program. The ~400K$ remaining funds were used at AFRL's consent to 1) migrate the security capabilities to Intel's next generation FPGA family – Agilex, 2) perform some research into hardware and software modification on future families to support certifiability of customer FPGA based solutions and 3) a system level demonstration of a subset of the security features used in a trusted execution enclave (TEE) using a Xeon processor and a Stratix 10 FPGA as an accelerator.

Intel has completed reports and presentations as per the agreed timeline demonstrating the capabilities of the Glen Pass security solutions.

Lastly, the goal of this program was to accelerate the development of these important security features. This program has the Stratix 10 features be completed in the two-year planned timeline in contrast to the ongoing delays due to development priorities. The features were made available five years after the Stratix 10 production silicon milestone. The work done has substantially accelerated the Agilex development to enable these features to become available coincident with the Agilex production silicon milestones, the earliest possible availability. This will enable developers in the defense industrial base to take advantage of these capabilities, enhancing hardware and software security years ahead of what would have been possible. Together, Intel and AFRL, we have made a difference!

Approved for public release. Distribution is unlimited.

6 APPENDIX A

Available User Guides

Intel Stratix 10 Device Security User Guide: https://www.intel.com/content/www/us/en/docs/programmable/683642/21-4/device-security-overview-s10-fm-dm.html

Intel Agilex Device Security User Guide: https://cdrdv2.intel.com/v1/dl/getContent/727747?explicitVersion=true , public web: https://www.intel.com/content/www/us/en/docs/programmable/683823/22-1/device-security-overview-s10-fm-dm.html

Also available for users under NDA:

Intel Agilex and Intel eASIC N5X HPS Cryptographic Services User Guide (document ID 728838)

Security Methodology for Intel FPGAs and Structured ASICs User Guide (document ID 724441)

Additional user guides/documentation will be available in Q3/Q4 2022, including:

Black Key Provisioning Service user guide

More detailed attestation chapters in the existing documentation.

"Security Methodology Companion Series", a training document which will have a Description, Overview, and Deep Dive section for each chapter of the Methodology document.

For any additional assistance with usage documentation or access, please contact Tony Cartolano: **tony.cartolano@intel.com**

LIST OF SYMBOLS, ABBREVIATIONS, AND ACRONYMS

Specific Program Abbreviations

FPGA	Field Programmable Gate Array
SoC	System on a chip
SDM	Secure Device Manager
LSM	Local Sector Manager
POF	FPGA configuration file used for programming the FPGA
PUF	Physical Unclonable Function
EMIB	Intel's embedded bridge technology for package integration of chiplets
NCLG	Networking and Custom Logic group (formerly PSG)
PSG	Programmable Solutions Group
SDL	Secure Design Cycle
PCL	Product Cycle Lifetime
AES	Most widely used encryption standard (Advanced Encryption Standard)
ECDSA	Elliptical Curve Signature Algorithm
SHA	Secure Hash Algorithm

General Acronyms and Abbreviations

Term/Acronym	Definition
AES	Most Widely Used Encryption Standard. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
AT	Anti-tamper. Mechanisms to deter, reverse engineering of critical technology, intelligent of system capabilities and prevent development of counter measures.
AT Monitor	Mechanisms to measure system characteristics such as voltage, temperature, etc. which can be used to determine if a tamper threat is present
AT Supervisor	Mechanism to evaluate inputs from AT Monitors and determine if an AT Event has occurred and an AT response is required
AT Event	The defined conditions for a Tamper response have been recognized by the AT Supervisor
AT Response	The systems response to an AT Event
Authenticity	Ensure information has come from the intended entity
Brainpool P Curve	A Prime Field Elliptical Curve recognized by European Government. http://www.ecc-brainpool.org/download/Domain-parameters.pdf
Confidentiality	Ensure information is readable only by the intended receiver

Approved for public release. Distribution is unlimited.

Term/Acronym	Definition
CSK	Code Signing Key. A Public Key use to validate integrity and Authenticity of a block of code. Typically Held in external flash and associated to enable key changes through key laddering.
DPA	Differential Power Analysis. A more advanced (Comparing with SPA) form of power analysis which can allow an attacker to compute the intermediate values within cryptographic computations by statistically analyzing data collected from multiple cryptographic operations.
EC(ECC)	Elliptic Curve. New PKI algorithm designed to replace RSA. We will use to EC in this document to avoid terminology collision with ECC which is as Error Control Coding unless otherwise stated
ECDSA	DSA algorithm using Elliptic Curve. https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm
ECDH	Diffie Hellman is an algorithm used to establish a shared secret between two parties. ECDH is Diffie-Hellman Key Exchange protocol using Elliptic Curve.
EMFI	Electromagnetic Fault Injection. It enables fault injection in small silicon region using strong electromagnetic pulse.
HMAC	In cryptography, a keyed-hash message authentication code (HMAC) is a specific type of message authentication code (MAC) involving a cryptographic hash function (hence the 'H') in combination with a secret cryptographic key.
Integrity	Ensure information has not been altered within each piece of information and among combination of difference pieces of information.
Invasive Debug	Any debug operation that might cause the behavior of the system to be modified such as Break Point.
Intrusive Physical Attack	Attacks require to make physical modification. There are multiple levels of this types of intrusive physical attack ranking from simple to complicate: Board Level, Package Level, and Chip Level. Example: Power Glitch – Board Level Physical Attack Top Metal Layer Probing – Package Level Attack FIBS – Chip level Physical Attack
Non-Invasive Debug	Any debug operation that might cause the behavior of the system not to be modified such as Trace.

Term/Acronym	Definition
Non-Intrusive Physical Attack	Attack doesn't require any physical modification. It is often considered as easier attacker than Intrusive Physical Attack. Example: SCA and EMFI
KAK	Key Authorization Key. A Public Key used to validate integrity and authenticity of another key
KDF	Key Derivation Function: http://csrc.nist.gov/groups/ST/toolkit/documents/kms/key-wrap.pdf
KEK	Key Encryption Key. http://csrc.nist.gov/groups/ST/toolkit/documents/kms/key-wrap.pdf
NIST P Curve	A list of NIST defined Elliptic Curve in Prime Field. P256 & P384 are used. Without anything specific information associated, P256/P384 means NIST P256/P364 Curves.
PUF	Physical Unclonable Function. It is a physical entity that is embodied in a physical structure and is easy to evaluate but hard to predict. Further, an individual PUF device must be easy to make but practically impossible to duplicate.
Root Key	Single Key that could traceable to finale security root for both confidentiality and authenticity
Root of Trust	A mechanism known to behave in an expected behavior which can describe the current trustworthiness of the associated system.
Security In Scope	Supported Security Threats
Security Out Scope	Not Supported Security Threats
SCA	Side Channel Attack. Any attacks relied on information leakage through un-intended channel could be classified as Side Channel. Example: SPA, DPA, EM, Acoustic, Cache Missing latency, and etc.
SDM	Secure Device Manager. Centralize Configuration Management Engine for Security and Configuration
SM2 P Curve	A Prime field Elliptic Curve defined by Chinese Government. http://www.oscca.gov.cn/UpFile/20101222214822692.pdf http://www.oscca.gov.cn/UpFile/20101222214836668.pdf
SPA	Simple Power Analysis. It involves visually interpreting power *traces*, or graphs of electrical activity over time.

Approved for public release. Distribution is unlimited.

Term/Acronym	Definition
Threat Vector	This defines adversary attack methods on scope security features
Transitive Trust	A mechanism to extend the trust boundary to functions beyond the Root of Trust
Trust	Expectation that a device will behave in a manner for a specific purpose

Approved for public release. Distribution is unlimited.