CSPN Security Target

HP Sure Start HW Root of Trust

NPCX998HB0

Revision Record

Revision	Date	Comments
1.0	June 27, 2022	First version

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Document Context

This document is intended to define the target of evaluation used for the ANSSI[1] defined CSPN[2] security certification framework for the "HP Sure Start – NPCX998HB0" microcontroller implemented by HP Inc.

1.2 Product Identification

Editor	HP Inc. 1501 Page Mill Road, Palo Alto, CA 94304 P.C. 94304-1112 Palo Alto United States
Link	http://www.hp.com
Products	The HP Sure Start NPCX998HB0 Microcontroller die in 144-Pin Very Thin Profile Fine-Pitch Ball Grid Array (VFBGA)
Part Number	NPCX998HB0BX
Chip Revision	02h
ROM Version	11.1.11.0
Products Category	Hardware and embedded software

Table 1 Evaluated product identification

1 Agence nationale de la sécurité et des systèmes d'information
2 Certification de Sécurité de Premier Niveau

2. TOE Summary Description

2.1 Identification

The Target of Evaluation (TOE) is the HP Sure Start microcontroller hardware component upon which HP Sure Start features of are built into HP platforms.

2.2 Feature

The TOE consists of hardware and software mechanisms designed to prevent unauthorized execution of low-level system firmware in a computing platform. This TOE is typically used in HP platform products to ensure that unauthorized modifications to system firmware (BIOS) do not go undetected and that they can be recovered automatically.

2.3 Architecture

The TOE consists of the following components

- A microcontroller with built-in cryptographic hardware functionality
- Software stored in ROM (Read-Only-Memory), inside the microcontroller
- Embedded SRAM (Static Random Access Memory), inside the microcontroller
- One Time Programmable memory (fused), inside the microcontroller
- The following Interfaces
    - A power line to receive power from the computer main board
    - A control line to connect to the chipset/CPU reset line on the computer main board
    - A memory access line to an External Flash Memory components which contains firmware to be loaded by the microcontroller

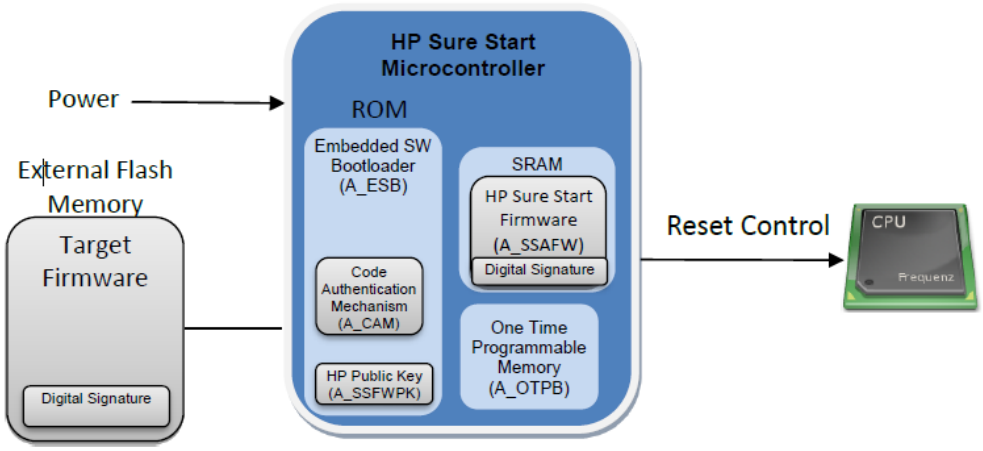

Figure 1 Target of Evaluation (TOE) Overview

The TOE acts as a hardware root of trust on the computer system where it is integrated. It is powered first when power is applied to the computer system, and it will ensure that only firmware appropriately authorized by the manufacturer will load into the HP Sure Start microcontroller before continuing with boot. This process uses digital signature verification in conjunction with an embedded public key and OTP memory (for key authorization policy) to ensure that the HP Sure Start microcontroller firmware is authentic. The TOE then becomes the root of trust for further functionality that will run on the HP Sure Start microcontroller, including verifying the authenticity of other components in the computer system.

This solution provides assurances to the computer user that the system will only boot with validated firmware in the TOE. This is designed to occur without requiring any action on the part of the user.

2.4 Assumptions

The overall solution assumes that cryptographic materials used to digitally signed authorized firmware updates are generated in a trusted environment controlled by the manufacturer (HP), whereby private portions of those materials never leave that trusted environment.
The solution is typically deployed in mass market end-user devices, such as PCs or printers.

3. Security Problem Definition

3.1 Assets

- An Embedded Software Bootloader (A_ESB): This software is used to boot the TOE HP Sure Start microcontroller when power is applied and the solution starts executing. Its integrity must be protected to ensure proper operation of the TOE.
- Code Authentication Mechanism (A_CAM): The A_CAM will validate the integrity and authenticity of the firmware code loaded by the A_ESB Bootloader.
- One-Time-Programmable memory bank (A_OTPB): OTP bits within the TOE that are used by the A_CAM and A_ESB to control code authentication policy parameters and that can retain their state in a reliable manner that is not reversible.
- HP Sure Start Authorized Firmware (A_SSAFW): Authorized HP Sure Start firmware code, including a digital signature issued by HP, which is intended to be loaded into SRAM by A_ESB and successfully validated using the A_CAM, according to A_OTPB policy settings, before subsequent execution by the TOE microcontroller.
- HP Sure Start Authorized Firmware Public Key (A_SSAFWPK): The Public key stored within A_ESB Embedded Software Bootloader used by A_CAM to authorize HP Sure Start firmware code.

The security requirements for the critical assets are the following:

Assets	Availability	Confidentiality	Integrity	Authenticity
An Embedded Software Bootloader (A_ESB)			X	
Code Authentication Mechanism (A_CAM)	X		X	
One-Time-Programmable memory bank (A_OTPB)			X	
HP Sure Start Authorized Firmware (A_SSAFW)			X	X
HP Sure Start Authorized Firmware Public Key (A_SSAFWPK)			X	

3.2 Threats

3.2.1 Replacement of Embedded Software Bootloader

An attacker manages to modify the microcontroller Embedded Software Bootloader (A_ESB) inside the microcontroller ROM, for example to bypass the code authentication mechanism (A_CAM), to ultimately load unauthorized firmware and execute it in the HP Sure Start microcontroller.

3.2.2 Code Signing Subversion

An attacker manages to modify the Target Firmware data in external Flash Memory in such a way that will bypass the code signing verification mechanism (A_CAM), and result in the loading of unauthorized firmware to run in the HP Sure Start microcontroller.

3.2.3 Policy Settings Alteration
An attacker manages to manipulate A_OTPB policy control bits in such a way that results in rolling back state to authorize the loading of firmware (by A_ESB) for which authorization had been previously revoked, and run it in the HP Sure Start microcontroller.

3.2.4 Crypto Attack
An attacker manages to attack the cryptographic algorithm implementation used in the TOE in order to forge a digital signature that will appear legitimate and resulting in the loading unauthorized firmware in the HP Sure Start microcontroller.

3.3 Security Functions
3.3.1 ROM based Integrity Protection
The TOE contains a true Read-Only-Memory which protects the integrity of the A_ESB Embedded Software Bootloader (inclusive of the A_CAM), and the HP Sure Start Authorized Firmware Public Key (A_SSAFWPK) against any modification.

3.3.2 Code Signature Verification
The TOE bootloader contains a code authentication (A_CAM) mechanism used to verify the both the integrity and the authenticity of a digital signature of the target firmware it loads from external flash memory before it is executed by the TOE.

3.3.3 OTP Based Integrity Protection
The TOE uses an One-Time-Programmable memory Bank (A_OTPB) to record the locking of specific TOE security parameters controlling the A_ESB for key authorization policy that is not reversible.

3.3.4 Availability of Code Authentication Mechanism
The TOE system design ensures that the Sure Start component is powered first and that the state of the component upon starting execution prevents the main CPU from starting execution, thus protecting against the possibility of an external agent attempting to execute code on the CPU in advance of A_CAM execution.

3.4 Cryptographic Properties
3.4.1 Crypto HW
The A_CAM uses a hardware implementation of cryptographic RSA verification, which will be used by the A_ESB Embedded Software Bootloader to reliably authenticate A_ASSFW Firmware that is loaded from external flash memory into A_SRAM before it is executed by the HP Sure Start microcontroller.

3.4.2 Key Sizes
The A_CAM is designed to verify RSA 3072 digital signature, using SHA384 hashing, according to the PKCS #1 v2.1 signature schemes RSASSA-PSS.

3.4.3 HP Public Key
The HP RSA 3072 Public Key (A_SSAFWPK) used by A_CAM to verify the digital signature for the HP Sure Start firmware is stored in permanent ROM memory inside the HP Sure Start microcontroller.