NIST SPECIAL PUBLICATION 1800-34B

Validating the Integrity of Computing Devices

Volume B:
Approach, Architecture, and Security Characteristics

Tyler Diamond
Nakia Grayson
William T. Polk
Andrew Regenscheid
Murugiah Souppaya
National Institute of Standards and Technology
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity
Clifton, Virginia

Christopher Brown
The MITRE Corporation
McLean, Virginia

August 2021

PRELIMINARY DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/building-blocks/supply-chain-assurance

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-34B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-34B, 51 pages, (August 2021), CODEN: NSPUE2

FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

Comments on this publication may be submitted to: supplychain-nccoe@nist.gov.

Public comment period: August 31, 2021, through September 29, 2021

As a private-public partnership, we are always seeking feedback on our practice guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at supplychain-nccoe@nist.gov.

All comments are subject to release under the Freedom of Information Act.

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

Organizations are increasingly at risk of cyber supply chain compromise, whether intentional or unintentional. Cyber supply chain risks include counterfeiting, unauthorized production, tampering, theft, and insertion of unexpected software and hardware. Managing these risks requires ensuring the integrity of the cyber supply chain and its products and services. This project will demonstrate how organizations can verify that the internal components of the computing devices they acquire, whether laptops or servers, are genuine and have not been tampered with. This solution relies on device vendors storing information within each device, and organizations using a combination of commercial off-the-shelf and open-source tools that work together to validate the stored information. This NIST

Cybersecurity Practice Guide provides a preliminary draft describing the work performed so far to build and test the full solution.

KEYWORDS

computing devices; cyber supply chain; cyber supply chain risk management (C-SCRM); hardware root of trust; integrity; provenance; supply chain; tampering.

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Charles Robison	Dell Technologies
Mukund Khatri	Dell Technologies
Rick Martinez	Dell Technologies
Daniel Carroll	Dell Technologies
Travis Raines	Eclypsium
John Loucaides	Eclypsium
Jason Cohen	Hewlett Packard Enterprise
CJ Coppersmith	Hewlett Packard Enterprise
Boris Balacheff	HP, Inc
Jeff Jeansonne	HP, Inc
Joshua Schiffman	HP, Inc
Tom Dodson	Intel

Name	Organization
Jason Ajmo	The MITRE Corporation
Chelsea Deane	The MITRE Corporation
Spike E. Dog	The MITRE Corporation
Joe Sain	The MITRE Corporation
Thomas Walters	The MITRE Corporation
Andrew Medak	National Security Agency (NSA)
Lawrence Reinert	NSA
Themistocles Chronis	RSA
Dan Carayiannis	RSA
Manuel Offenberg	Seagate
David Kaiser	Seagate
Paul Gatten	Seagate
Simon Phatigaraphong	Seagate
Bill Downer	Seagate Government Solutions
Jack Fabian	Seagate Government Solutions

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
Dell Technologies	PowerEdge R650, Secured Component Verification tool; Precision 3530, CSG Secured Component Verification tool
Eclypsium	Eclypsium Analytics Service, Eclypsium Device Scanner
HP Inc.	(2) Elitebook 840 G7, HP Sure Start, HP Sure Recover
Hewlett Packard Enterprise	Proliant DL360
Intel	HP, Inc Elitebook 360 830 G5, Lenovo ThinkPad T480, Transparent Supply Chain Tools, Key Generation Facility, Cloud Based Storage, TSCVerify and Autoverify software tools
RSA	RSA Archer Suite 6.9
Seagate Government Solutions	(3) 18TB Exos X18 hard drives, Firmware Attestation API, Secure Device Authentication API
National Security Agency (NSA)	Host Integrity at Runtime and Start-up (HIRS), Subject Matter Expertise

DOCUMENT CONVENTIONS

The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms “should” and “should not” indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms

"may" and "need not" indicate a course of action permissible within the limits of the publication. The terms "can" and "cannot" indicate a possibility and capability, whether material, physical, or causal.

CALL FOR PATENT CLAIMS

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
2. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: supplychain-nccoe@nist.gov

Contents

1 Summary 1

1.1 Challenge 2

1.2 Solution 3

1.3 Benefits 4

2 How to Use This Guide 4

2.1 Typographic Conventions 5

3 Approach 6

3.1 Audience 6

3.2 Scope 7

3.2.1 Scenario 1: Creation of Verifiable Platform Artifacts 7

3.2.2 Scenario 2: Verification of Components During Acceptance Testing 7

3.2.3 Scenario 3: Verification of Components During Use 7

3.3 Assumptions 8

3.4 Risk Assessment 8

3.4.1 Threats 9

3.4.2 Vulnerabilities 10

3.4.3 Risk 11

3.5 Security Control Map 13

3.6 Technologies 14

3.6.1 Trusted Computing Group 16

4 Architecture 16

4.1 Architecture Description 17

4.2 Existing Enterprise IT Management Systems 19

4.2.1 Asset Discovery and Management System 19

4.2.2 Configuration Management System 20

4.3 Supporting Platform Integrity Validation Systems 22

133 4.3.1 Host Integrity at Runtime and Start-up Attestation Certificate Authority
134 (HIRS ACA) 22
135 4.3.2 Network Boot Services 23
136 4.3.3 Platform Manifest Correlation System 24
137 4.3.4 Eclypsium Analytic Platform 25
138 4.4 Computing Devices 27
139 4.4.1 HP Inc. 27
140 4.4.2 Dell Technologies 29
141 4.4.3 Intel 29
142 **5 Security Characteristic Analysis 31**
143 5.1 Assumptions and Limitations 31
144 5.2 Build Testing 31
145 5.2.1 Scenario 1 31
146 5.2.2 Scenario 2 34
147 5.2.3 Scenario 3 39
148 5.3 Scenarios and Findings 40
149 5.3.1 Supply Chain Risk Management (ID.SC) 40
150 5.3.2 Asset Management (ID.AM) 41
151 5.3.3 Identity Management, Authentication and Access Control (PR.AC) 41
152 5.3.4 Data Security (PR.DS) 41
153 5.3.5 Security Continuous Monitoring (DE.CM) 41
154 **6 Future Build Considerations 42**
155 **Appendix A List of Acronyms 43**
156 **Appendix B References 45**
157 **Appendix C Project Scenario Sequence Diagrams 47**

158 # List of Figures

159 **Figure 1-1 Supply Chain Risk 2**

Figure 4-1 Notional Architecture 17
Figure 4-2 Component-Level Architecture 18
Figure 4-3 HIRS ACA Platform 23
Figure 4-4 Network Boot Services Environment 24
Figure 4-5 Platform Manifest Correlation System 25
Figure 4-6 Eclypsium Management Console 26
Figure 4-7 Eclypsium Analytics Platform 27
Figure 5-1 Platform Certificate Binding to Endorsement Credential 32
Figure 5-2 Intel Transparent Supply Chain Download Portal 35
Figure 5-3 HIRS ACA Validation Dashboard 36
Figure 5-4 Asset Inventory and Discovery Example 1 38
Figure 5-5 Asset Inventory and Discovery Example 2 38
Figure 5-6 Scenario 3 Dashboard 40
Figure 6-1 Dell Laptop Scenario 2 Part 1 47
Figure 6-2 Dell Laptop Scenario 2 Part 2 48
Figure 6-3 Intel Laptop Scenario 2 Part 1 49
Figure 6-4 Intel Laptop Scenario 2 Part 2 50
Figure 6-5 Intel Laptop Scenario 3 51

List of Tables

Table 3-1 NIST SP 800-161 Threat Events 9
Table 3-2 C-SCRM Example Threat Scenario 12
Table 3-3 Security Characteristics 13
Table 3-4 Security Characteristics and Controls Mapping 14
Table 3-5 Products and Technologies 15
Table 5-1 Prototype Platform Artifact 33

1 Summary

Organizations are increasingly at risk of cyber supply chain compromise, whether intentional or unintentional. Cyber supply chain risks include counterfeiting, unauthorized production, tampering, theft, and insertion of unexpected software and hardware. Managing these risks requires ensuring the integrity of the cyber supply chain and its products and services. This prototype implementation will demonstrate how organizations can verify that the internal components of the computing devices they acquire are genuine and have not been unexpectedly altered during manufacturing or distribution processes.

This is a preliminary draft of the document, and while the content is considered to be stable, changes are expected to occur. There are gaps in the content and the overall document is still incomplete. This guide includes proof-of-concept software tools and services which have not been commercialized by our partner collaborators. NIST welcomes early informal feedback and comments, which will be adjudicated after the specified public comment period. Organizations may consider experimenting with guidelines, with the understanding that they will identify gaps and challenges.

This project will be conducted in two phases: laptop and server builds. This preliminary draft focuses on securing laptop hardware contributed by our technology partners. In a future version of this publication, we will incorporate hardware from our server manufacturing partners. The server builds will leverage much of the laptop build architecture that is documented in this practice guide. We hope that this approach will provide organizations a holistic methodology to managing supply chain risk.

For ease of use, the following provides a short description of each section in this volume.

Section 1, Summary, presents the challenge addressed by this NCCoE project, including our approach to addressing the challenge, the solution demonstrated, and the benefits of the solution.

Section 2, How to Use This Guide, explains how business decision makers, program managers, and information technology (IT) and operational technology (OT) professionals might use each volume of the guide.

Section 3, Approach, offers a detailed treatment of the scope of the project, the risk assessment that informed the solution, and the technologies and components that industry collaborators supplied to build the example solution.

Section 4, Architecture, specifies the components of the prototype implementation and details how data and communications flow between validation systems.

Section 5, Security Characteristic Analysis, provides details about the tools and techniques used to test and understand the extent to which the project prototype implementation meets its objective: demonstrating how organizations can verify that the components of their acquired computing devices are genuine and have not been tampered with or otherwise modified throughout the devices' life cycles.

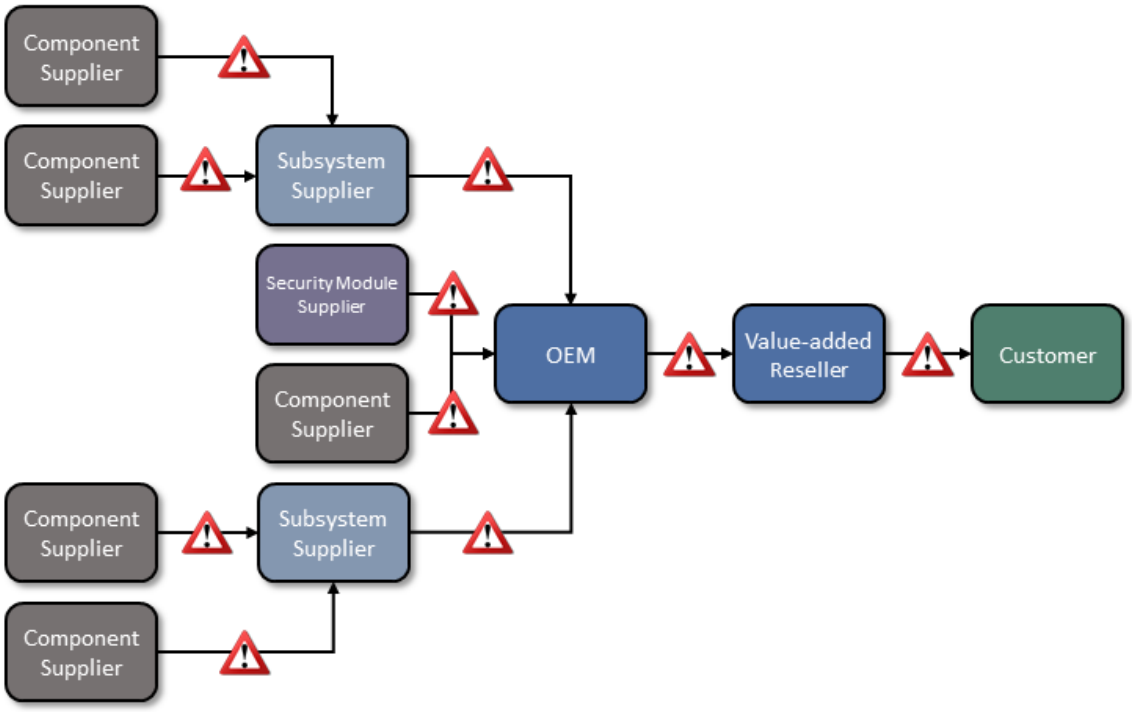
Section 6, Future Build Considerations, conveys the technical characteristics we plan to incorporate as we continue to prototype with our collaborators.

Appendices A through C provide acronyms, a list of references cited in this volume, and project scenario sequence diagrams, respectively.

1.1 Challenge

Technologies today rely on complex, globally distributed and interconnected supply chain ecosystems to provide highly refined, cost-effective, and reusable solutions. Most organizations' security processes consider only the visible state of computing devices. The provenance and integrity of a delivered device and its components are typically accepted without validating through technology that there have been no unexpected modifications. *Provenance* is the comprehensive history of a device throughout the entire life cycle from creation to ownership, including changes made within the device or its components. Assuming that all acquired computing devices are genuine and unmodified increases the risk of a compromise affecting products in an organization's supply chain, which in turn increases risks to customers and end users, as illustrated in Figure 1-1. Mitigating this risk is not addressed at all in many cases.

Figure 1-1 Supply Chain Risk



Organizations currently lack the ability to readily distinguish trustworthy products from others. At best, government organizations could access an information source on counterfeit components such as the Government-Industry Data Exchange Program (GIDEP), which contains information on equipment, parts, and assemblies that are suspected to be counterfeit. Additionally, organizations with sufficient resources could have acquisition quality assurance programs that examine manufacturer supply chain practices, perform spot-checks of deliveries, and/or require certificates of conformity.

Having this ability is a critical foundation of cyber supply chain risk management (C-SCRM). *C-SCRM* is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of supply chains. C-SCRM presents challenges to many industries and sectors, requiring a coordinated set of technical and procedural controls to mitigate cyber supply chain risks throughout manufacturing, acquisition, provisioning, and operations.

1.2 Solution

To address these challenges, the NCCoE is collaborating with technology vendors to develop a prototype implementation. Once completed, this project [1] will demonstrate how organizations can verify that the internal components of the computing devices they acquire are genuine and have not been tampered with. This solution relies on device vendors storing information within each device, and organizations using a combination of commercial off-the-shelf and open-source tools that work together to validate the stored information. By doing this, organizations can reduce the risk of compromise to products within their supply chains.

In this approach, device vendors create one or more artifacts within each device that securely bind the device's attributes to the device's identity. An organization who acquires the device can validate |the artifacts' source and authenticity, then check the attributes stored in the artifacts against the device's actual attributes to ensure they match before fielding the device to the end user. A similar process can be used to verify the integrity of computing devices while they are in use.

Hardware roots of trust are a central technology in our approach to enable the use of authoritative information regarding the provenance and integrity of the components, which provide a strong basis for trust in a computing device. A hardware root of trust is comprised of highly reliable firmware and software components that perform specific, critical security functions. Hardware roots of trust are the foundation upon which the computing system's trust model is built, forming the basis in hardware for providing one or more security-specific functions for the system. By leveraging hardware roots of trust as a computing device traverses the supply chain, we can maintain trust in the computing device throughout its operational lifecycle.

This project will address several processes, including:

- how to create verifiable descriptions of components and platforms, which may be done by original equipment manufacturers (OEMs), platform integrators, and even IT departments;

- how to verify the integrity and provenance of computing devices and components within the single transaction between an OEM and a customer; and
- how to continuously monitor the integrity of computing devices and components at subsequent stages in the system lifecycle in the operational environment.

1.3 Benefits

This practice guide can help organizations, including but not limited to OEMs and third-party component suppliers, to:

- avoid using compromised technology components in your products
- enable customers to readily verify that OEM products are genuine and trustworthy
- prevent compromises of your organization's information and systems caused by acquiring and using compromised technology products

2 How to Use This Guide

This is a preliminary draft of Volume B of a NIST Cybersecurity Practice Guide. Implementation of the prototype implementation at the NCCoE is ongoing. The NCCoE is providing this preliminary draft to gather valuable feedback and inform stakeholders of the progress of the project. Organizations should not attempt to implement this preliminary draft.

When finalized, this NIST Cybersecurity Practice Guide will demonstrate a standards-based reference design for verifying that the internal components of the computing devices organizations acquire are genuine and have not been tampered with, and provide readers with the information they need to replicate the reference design. It is modular and can be deployed in whole or in part.

This guide will contain three volumes:

- NIST SP 1800-34A: *Executive Summary*
- NIST SP 1800-34B: *Approach, Architecture, and Security Characteristics* – what we built and why **(you are here)**
- NIST SP 1800-34C: *How-To Guides* – instructions for building the example solution

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary, NIST SP 1800-34A*, which describes the following topics:

- challenges that enterprises face in decreasing the risk of a compromise to products in their supply chain
- example solution built at the NCCoE

- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, *NIST SP 1800-34B*, which describes what we did and why. The following sections will be of particular interest:

- Section 3.4, Risk, provides a description of the risk analysis we performed
- Section 3.4.3.1, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices

You might share the *Executive Summary, NIST SP 1800-34A*, with your leadership team members to help them understand the importance of adopting a standards-based method for verifying that the internal components of the computing devices they acquire are genuine and have not been tampered with.

IT professionals who want to implement an approach like this will find the whole practice guide useful. Once the how-to portion of the guide, *NIST SP 1800-34C*, is complete, you will be able to use it to replicate all or parts of the build created in our lab. The how-to portion of the guide will provide specific product installation, configuration, and integration instructions for implementing the example solution. We will not re-create the product manufacturers' documentation, which is generally widely available. Rather, we will show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial and open-source products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a prototype implementation for verifying that the internal components of the computing devices your organization acquires are genuine and have not been tampered with. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.6, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a preliminary draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to supplychain-nccoe@nist.gov.

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the *NCCoE Style Guide*.
Bold	names of menus, options, command buttons, and fields	Choose **File** > **Edit**.
`Monospace`	command-line input, onscreen computer output, sample code examples, and status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at https://www.nccoe.nist.gov.

3 Approach

Organizations currently lack the ability to readily distinguish trustworthy products from others. To address this challenge, the NCCoE proposes an adaptable prototype implementation that organizations can use to verify that the internal components of the computing devices they acquire are genuine and have not been tampered with. The NCCoE leveraged the existing ongoing initiatives by the NIST C-SCRM program, including workshop research findings and use case studies, that sought input from technology and cybersecurity vendors, C-SCRM subject matter experts from academia, and government to define the project scope and reference architecture.

This guide describes a proof-of-concept implementation of the approach—a prototype—that is intended to be a blueprint or template for the general security community. It is important to note that the prototype implementation presented in this publication is only one possible way to solve the security challenges. It is not intended to preclude the use of other products, services, techniques, etc. that can also solve the problem adequately, nor is it intended to preclude the use of any products or services not specifically mentioned in this publication.

3.1 Audience

This guide is intended for organizations and individuals who are responsible for the acquisition, provisioning, and configuration control of computing devices. Examples include IT administrators/system administrators, incident response team members, and Security Operations Center staff. OEMs, value-added resellers (VARs), and component suppliers may also benefit from the prototype and lessons-learned at the conclusion of this project.

3.2 Scope

The scope of the project is limited to manufacturing and OEM processes that protect against counterfeits, tampering, and undocumented changes to firmware and hardware, and the corresponding customer processes that verify that client and server computing devices and components have not been tampered with or otherwise modified. Protection against undocumented changes to the operating system is considered out of scope for this project. Manufacturing processes that cannot be verified by the customer are also explicitly out of scope.

Further, this project is not intended to cover the entire supply chain risk management process; it will focus on the acceptance testing portion of a more holistic defense-in-depth/defense-in breadth supply chain risk management strategy. The project will enable verification of the identity of computing devices (including replacement parts and updates or upgrades) once they have been acquired but before they are implemented or installed.

Finally, this preliminary draft only documents our experiences with laptop (end user) computing devices in a Windows 10 environment. In our project roadmap (see Section 6), we plan to add servers that use Linux and Windows Server to the scope of the prototype. From this perspective, we have defined the following three project scenarios which outline the prototype scope.

3.2.1 Scenario 1: Creation of Verifiable Platform Artifacts

An OEM, VAR, or other authoritative source creates a verifiable artifact that binds reference platform attributes to the identity of the computing device. The platform attributes in this artifact (e.g., serial number, embedded components, firmware and software information, platform configuration) are used by the purchasing organization during acceptance and provisioning of the computing device. Customers may also create their own platform artifacts to establish a baseline that could be used to validate devices in the field.

3.2.2 Scenario 2: Verification of Components During Acceptance Testing

In this scenario, an IT administrator receives a computing device through non-verifiable channels (e.g., off the shelf at a retailer) and wishes to confirm its provenance and authenticity as part of acceptance testing to establish an authoritative asset inventory as part of an asset management program.

3.2.3 Scenario 3: Verification of Components During Use

In this scenario, the computing device has been accepted by the organization (Scenario 2) and has been provisioned for the end user. The computing device components are verified against the attributes and measurements declared by the manufacturer or purchasing organization during operational usage.

3.3 Assumptions

This project is guided by the following assumptions:

- The scenario activities above will augment, not replace, the capabilities of existing acceptance testing tools, asset management systems, and configuration management systems.
- Hardware roots of trust represent one technique that can thwart the above types of attacks to the supply chain. However, OEMs may use different approaches to implement a hardware root of trust solution because of hardware constraints or other business reasons.
- Organizational computing devices lifecycle phases for technology include the following activities defined in NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations [2]: integration (referred to as acceptance testing in this demonstration), operations, and disposal.

3.4 Risk Assessment

NIST Special Publication (SP) 800-30 Revision 1, Guide for Conducting Risk Assessments [2], states that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." The guide further defines risk assessment as "the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."

The NCCoE recommends that any discussion of supply chain risk management should begin with a comprehensive review of NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations [2]—publicly available material. While SP 800-161 is targeted to U.S. federal agencies, much of the guidance is beneficial to private organizations interested in reducing Information and Communications Technology (ICT) supply chain risk. NIST SP 800-161 defines an *ICT supply chain compromise* as an occurrence within the ICT supply chain whereby an adversary jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits. An ICT supply chain compromise can occur anywhere within the system development life cycle of the product or service.

In addition, NIST SP 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations [4] provides Risk Management Framework guidance that gives a baseline to assess risks to information system assets, including threats to the IT system supply chain.

3.4.1 Threats

NIST SP 800-161 provides a framework of ICT supply chain threats including insertion of counterfeits, unauthorized production, tampering, theft, or insertion of malicious software and hardware, as well as poor manufacturing and development practices in the ICT supply chain. These threats are associated with an organization's decreased visibility into, and understanding of, how the technology that it acquires is developed, integrated, and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services. Exploits created by malicious actors (individuals, organizations, or nation states) are often especially sophisticated and difficult to detect, and thus are a significant risk to organizations. This prototype implementation does not defend against all ICT threats, but Table 3-1 captures threats from NIST SP 800-161 that are relevant to this project.

Table 3-1 NIST SP 800-161 Threat Events

Threat Events	Description
Craft attacks specifically based on deployed IT environment.	Adversary develops attacks (e.g., crafts targeted malware) that take advantage of knowledge of the organizational IT environment.
Create counterfeit/spoof website.	Adversary creates duplicates of legitimate websites; when users visit a counterfeit site, the site can gather information or download malware.
Craft counterfeit certificates.	Adversary counterfeits or compromises a certificate authority so that malware or connections will appear legitimate.
Create and operate false front organizations to inject malicious components into the supply chain.	Adversary creates false front organizations with the appearance of legitimate suppliers in the critical life cycle path that then inject corrupted/malicious information system components into the organizational supply chain.
Insert counterfeit or tampered hardware into the supply chain.	Adversary intercepts hardware from legitimate suppliers. Adversary modifies the hardware or replaces it with faulty or otherwise modified hardware.
Insert tampered critical components into organizational systems.	Adversary replaces, through supply chain, subverted insider, or some combination thereof, critical information system components with modified or corrupted components.
Compromise design, manufacture, and/or distribution of information system components (including hardware, software, and firmware).	Adversary compromises the design, manufacture, and/or distribution of critical information system components at selected suppliers.

Threat Events	Description
Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware.	Adversary targets and compromises the operation of software (e.g., through malware injections), firmware, and hardware that perform critical functions for organizations. This is largely accomplished as supply chain attacks on both commercial off-the-shelf and custom information systems and components.
Obtain unauthorized access.	Adversary with authorized access to organizational information systems gains access to resources that exceeds authorization.
Inadvertently introduce vulnerabilities into software products.	Due to inherent weaknesses in programming languages and software development environments, errors and vulnerabilities are introduced into commonly used software products.

3.4.2 Vulnerabilities

This document is guided by NIST SP 800-161 [2], which describes an ICT supply chain vulnerability as the following:

> "A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source [FIPS 200], [NIST SP 800-34 Rev. 1], [NIST SP 800-53 Rev 4], [NIST SP 800-53A Rev. 4], [NIST SP 800-115]. Within the ICT SCRM context, it is any weakness in the system/component design, development, manufacturing, production, shipping and receiving, delivery, operation, and component end-of life that can be exploited by a threat agent. This definition applies to both the systems/components being developed and integrated (i.e., within the SDLC) and to the ICT supply chain infrastructure, including any security mitigations and techniques, such as identity management or access control systems. ICT supply chain vulnerabilities may be found in:
>
> - The systems/components within the SDLC (i.e., being developed and integrated);
> - The development and operational environment directly impacting the SDLC; and
> - The logistics/delivery environment that transports ICT systems and components (logically or physically)."

In the context of this project, ICT products (including libraries, frameworks, and toolkits) or services originating anywhere (domestically or abroad) might contain vulnerabilities that can present opportunities for ICT supply chain compromises. For example, an adversary may have the power to insert a malicious component into a product. While it is important to consider all ICT vulnerabilities, in practice it is impossible to completely eliminate all of them. Therefore, organizations should prioritize vulnerabilities that may have a greater impact on their environment if exploited by an adversary.

Additionally, a goal of this prototype implementation is to document a capability that enables organizations to detect the exploitation of vulnerabilities that may exist in firmware over-the-air processes that would allow an attacker to gain a privileged position on the computing device. In this

project, we introduce a continuous monitoring component within system firmware that organizations can incorporate into their continuous monitoring programs.

3.4.3 Risk

SP 800-161 provides an analysis framework for organizations to assess supply chain risk by creating a *threat scenario*—a summary of potential consequences of the successful exploitation of a specific vulnerability or vulnerabilities by a threat agent. By performing this exercise, organizations can identify areas requiring increased controls. Here, we walk through a truncated example scenario that may be similar to a threat scenario faced by organizations who implement some or all parts of this prototype demonstration. Readers are encouraged to develop their own threat scenario assessment for their organization as part of a larger risk management program.

3.4.3.1 Threat Scenario

A company purchases life cycle replacement network hardware from a third-party VAR with whom it has done business in the past. The business side of the company is pressuring the IT Operations staff to rapidly replace the network infrastructure off-hours to avoid downtime during regular business hours. The IT department responds by accelerating its deployment schedule to nights and weekends, using existing staff augmented with VAR technicians.

Following deployment of the new hardware, the IT department observes that network performance is actually slower in the subnets where the equipment has been installed. Two weeks of network performance tests are conducted to validate the network issues, culminating with a report that the new hardware is actually 25% slower than the previous hardware.

At the same time, the company's Information Security department notices unusual traffic coming from computers in the upgraded subnets. Their investigation finds that some computers in the affected subnets are beaconing out to international IP addresses where the company has no business presence or need. The computers generating the suspicious traffic are taken offline for further investigation.

The VAR is called, and their technicians perform a separate network traffic analysis, confirming the reduction in traffic speed. The VAR launches an investigation into the source of the network hardware that they sold to the company and finds that the equipment in question, as well as a portion of their existing stock of hardware, is counterfeit. The VAR sends a counterfeit network device to a security company for analysis. The security company finds that in addition to counterfeit hardware and substandard components, embedded malware has been installed, enabling attackers to take control of the network devices and to deliver second-stage malware that enabled them to move laterally through the affected subnets and compromise computers of interest. This also gave the attackers a persistent foothold inside the company.

An internal audit finds multiple failures on the part of the purchasing department, the IT department, and the Information Security group to have in place measures to ensure the provenance of the equipment and the secure deployment of devices on the network.

As a result of the supply chain breach leading to the installation of compromised hardware, the company suffered several adverse effects, including:

- loss of intellectual property through data exfiltration
- loss of employee productivity as a result of computers and network equipment being taken offline
- additional costs to the IT department for replacement computers and network equipment
- loss of confidence with the company's client base
- potential loss of revenue due to clients severing their relationship with the company

Consequently, the organization develops three mitigation strategies to address the identified risks, in which two are chosen as shown in Table 3-2. One of the chosen strategies, *Increase provenance and information requirements*, can be at least partially addressed by the final implementation of this project. Table 3-2 presents a summary of an example threat scenario analysis framework that an organization may use to determine the controls to implement that would cause the estimated residual risk of counterfeit hardware to drop to an acceptable level.

Table 3-2 C-SCRM Example Threat Scenario

Threat Scenario	Threat Source:	Industrial espionage/cyber criminals
	Vulnerability:	Internal: Loss of intellectual property following system compromise
	Threat Event Description:	Counterfeit hardware with embedded malware introduced into company's network
	Existing Practices:	Hardware system test prior to deployment; network scanning
	Outcome:	Data exfiltration, system degradation, loss of productivity, loss of revenue
Risk	Impact:	30% chance of successful targeting and infiltration
	Likelihood:	40% chance of undetected compromise
	Risk Score (Impact x Likelihood):	High
	Acceptable Level of Risk:	Low (under 25%)

Mitigation	Potential Mitigating Strategies/ SCRM Controls:	1) Improve traceability capabilities 2) Increase provenance and information requirements 3) Choose another supplier
	Estimated Cost of Mitigating Strategies:	1) Cost 20% increase, impact 10% decrease 2) Cost 20% increase, impact 20% decrease 3) Cost 40% increase, impact 80% decrease
	New Risk Score:	Low
	Selected Strategies:	2) Increase provenance and information requirements 3) Choose another supplier
	Estimated Residual Risk:	10%

3.5 Security Control Map

The following tables map the security characteristics defined in our project description (Table 3-3) to the applicable NIST Cybersecurity Framework [5] Functions, Categories, and Subcategories (Table 3-4) to assist organizations better manage and reduce C-SCRM risk. We have also included a mapping to specific SP 800-53 r4 security controls [6] and indicated (in bold) if the control is part of the SP 800-161 baseline security controls to assist organizations interested in alignment with NIST C-SCRM best practices.

Table 3-3 Security Characteristics

Identifier	Security Characteristic
1	Establish a strong device identity to support binding artifacts to a specific device.
2	Cryptographically bind platform attributes and other manufacturing information to a given computer system.
3	Establish assurance for multi-supplier production in which components are embedded at various stages.
4	Provide an acceptance test capability that validates source and integrity of assembled components for the recipient organization of the computer system.
5	Detect unexpected component (firmware) swaps or tampering during the life cycle of the computing device in an operational environment.

508 **Table 3-4 Security Characteristics and Controls Mapping**

Cybersecurity Framework v1.1			SP 800-53 R4	Security Characteristics Addressed
Function	**Category**	**Subcategory**		
Identify (ID)	Supply Chain Risk Management (ID.SC)	ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	**AU-2**	5
			AU-6	5
			SA-19	1,3
	Asset Management (ID.AM)	ID.AM-1: Physical devices and systems within the organization are inventoried.	**CM-8**	4
			AU-10	4
Protect (PR)	Identity Management, Authentication and Access Control (PR.AC)	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	**IA-4**	1
	Data Security (PR.DS)	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	SI-7	4,5
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.	**SA-10**	4,5
			SA-18	1
Detect (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	**PE-20**	5

509 ## 3.6 Technologies

510 Table 3-5 lists all of the technologies used in this project, and provides a mapping among the generic
511 component term, the specific product or technology used, the function or capability it provides, and the
512 Cybersecurity Framework Subcategories that the product helps support. Refer to Table 3-4 for an
513 explanation of the NIST Cybersecurity Framework Subcategory codes.

514 **Table 3-5 Products and Technologies**

Component	Product/Technology	Function/Capability	Cybersecurity Framework Subcategories
Component or Subsystem Manufacturer	Intel Transparent Supply Chain	Tools and processes to ensure supply chain security from the manufacturer to the purchasing organization	ID.SC-4, PR.DS-6
	Seagate EXOS X18 18 Terabyte Hard Drive	Secure device authentication, firmware attestation	ID.SC-4, PR.AC-6, PR.DS-6, PR.DS-8
OEM or VAR	Dell Technologies	Manufactures computing devices and binds them to verifiable artifacts	ID.SC-4
	Hewlett Packard Enterprise		
	HP Inc.		
	Lenovo		
Computing Device	Dell PowerEdge R640 Server	A client device (laptop) or server purchased by an organization to execute tasks by end users	ID.SC-4, PR.AC-6
	Dell Precision 3530		
	HPE ProLiant DL360		
	HP Inc. Elitebook 360 830 G5		
	HP Inc. 840 G7		
	Intel Server Board S2600WTT		
	Lenovo ThinkPad T480		
Asset Discovery and Management System	RSA Archer	Ensures computing devices and associated components are tracked and uniquely identified	ID.AM-1
Configuration Management System	Microsoft Configuration Manager	Enforces corporate governance and policies through actions such as applying software patches and updates, removing denylisted software, and automatically updating configurations	DE.CM-7
Security Information and Event Management Tool	RSA Archer	Real-time analysis of alerts and notifications generated by organizational information systems	DE.CM-7

Component	Product/Technology	Function/Capability	Cybersecurity Framework Subcategories
Certificate Authority	HIRS ACA	Issues an Attestation Identity Credential in accordance with TCG specifications	PR.AC-6, PR.DS-8
Platform Integrity Validation System	Eclypsium Analytic Platform	Validates the integrity of firmware installed on computing devices	PR.DS-6
	HIRS ACA	Validates platform components in accordance with TCG specifications	PR.DS-8
	Platform Manifest Correlation System	Ingests platform manifest data from participating manufacturers	ID.AM-1

3.6.1 Trusted Computing Group

The technology providers for this prototype implement standards from the TCG, a not-for-profit organization formed to develop, define, and promote open, vendor-neutral, global industry standards supportive of hardware-based roots of trust for interoperable trusted computing platforms. TCG developed and maintains the Trusted Platform Module (TPM) 2.0 specification [8], which defines a cryptographic microprocessor designed to secure hardware by integrating cryptographic keys and services [3]. A TPM functions as a root of trust for storage, measurement, and reporting. TPMs are currently included in many computing devices.

This project applies this foundational technology to address the challenge of operational security by verifying the provenance of a delivered system from the time it leaves the manufacturer until it is introduced in the organization's operational environment. The TPM can be leveraged to measure and validate the state of the system, including:

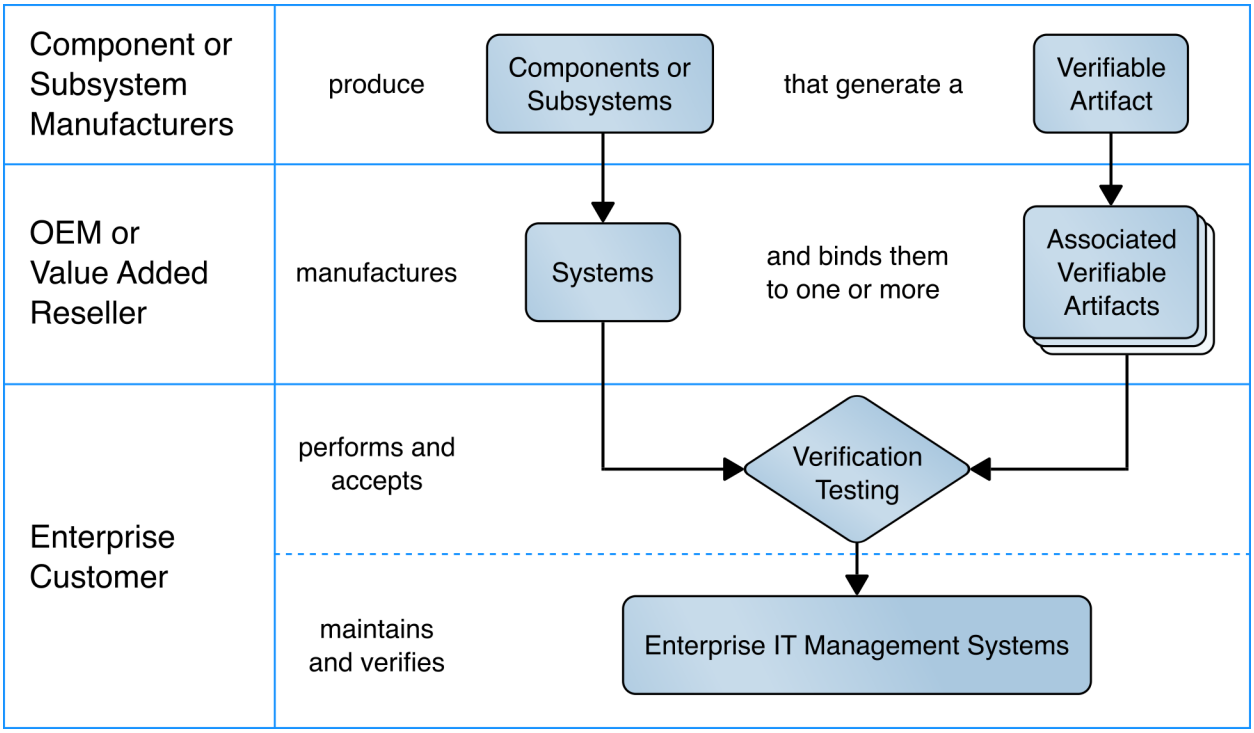
- binding attributes about the computing device to a strong cryptographic device identity held by the TPM, and
- supporting measurement and attestation capabilities that allow an organization to inspect and verify device components and compare them to those found in the platform attribute credential and OEM-provided reference measurements.

4 Architecture

This project is based on the notional high-level architecture depicted in Figure 4-1 for an organization incorporating C-SCRM technologies into its existing infrastructure. The architecture depicts a

manufacturer that creates a hardware-root-of-trust-backed verifiable artifact associated with a computing device. The verifiable artifact is then associated with existing enterprise IT management systems, such as asset and configuration management systems, during the provisioning process. Finally, an inspection component measures and reports on hardware attributes and firmware measurements during acceptance testing and operational use.

Figure 4-1 Notional Architecture



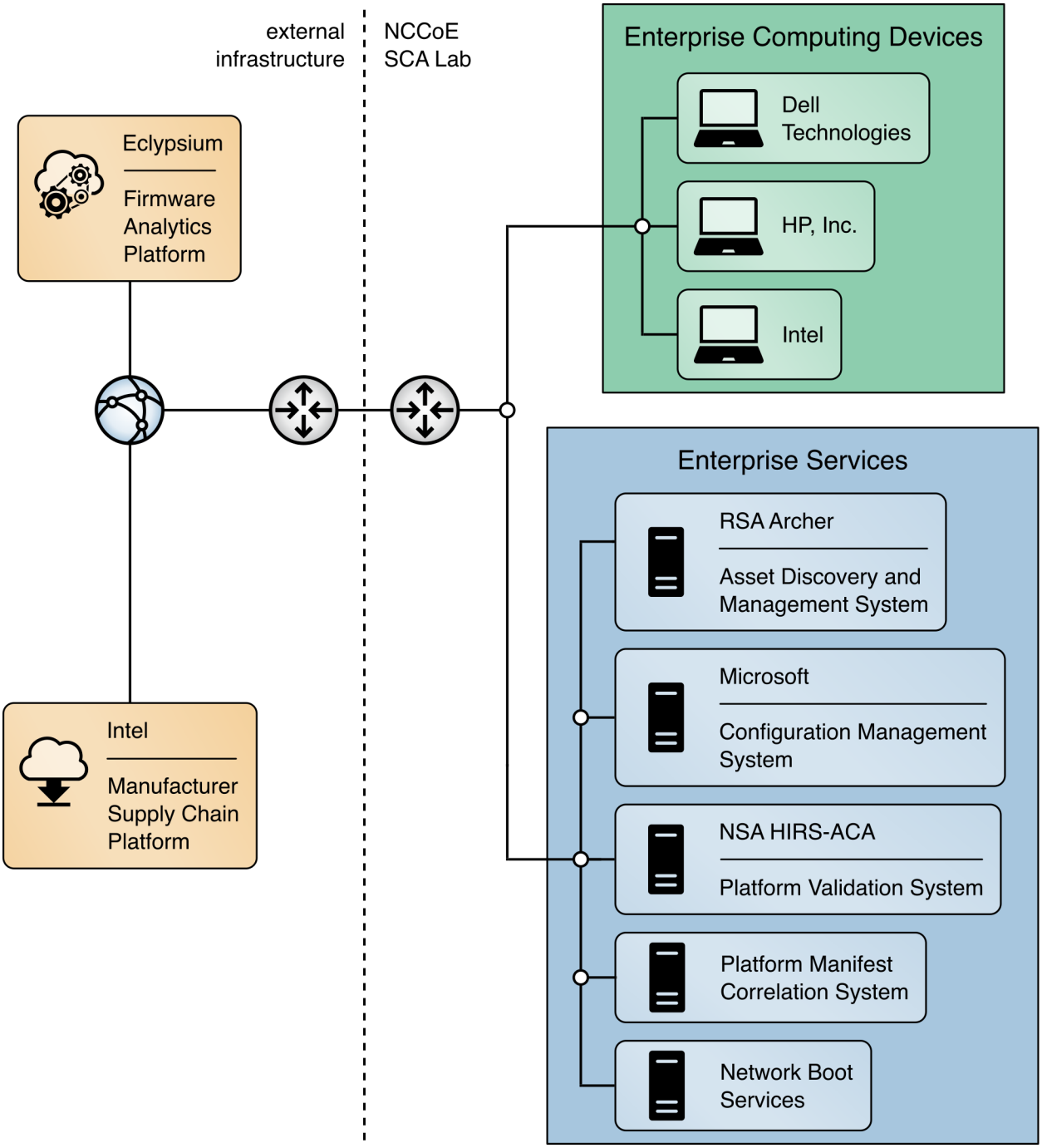
4.1 Architecture Description

The prototype architecture consists of two focus areas: 1) an implementation of a manufacturer that creates a hardware-root-of-trust-backed verifiable artifact associated with a computing device, and 2) the representational architecture of an organization where end users are issued computing devices that require access to enterprise services for initial acceptance testing of the device and operational validation of the platform.

This prototype implementation combines on-premises software, cloud platforms, and end user hardware to demonstrate the security characteristics defined in the project description (Table 3-3). Figure 4-2 presents a component-level view of the current prototype. The remaining sections discuss the existing IT components an organization may have deployed before the prototype has been implemented

551 and how they can be augmented to support a hardware integrity validation capability. They also discuss
552 additional services and platforms that are integrated into the enterprise architecture.

553 **Figure 4-2 Component-Level Architecture**



4.2 Existing Enterprise IT Management Systems

This prototype solution aims to augment, not replace, the capabilities of existing acceptance testing tools, asset management systems, and configuration management systems. In this iteration of the solution, this example enterprise uses an asset and configuration management system in the normal course of computing device acceptance. This section describes the functions of each system before and after the integration of the security characteristics defined in Section 3.4.3.1.

4.2.1 Asset Discovery and Management System

SP 800-128 [7] states that a *system component* is a discrete identifiable IT asset that represents a building block of a system. An accurate component inventory is essential to record the components that compose the system. The component inventory helps to improve the security of the system by providing a comprehensive view of the components that need to be managed and secured. The organization can determine the granularity of the components, and in the context of this prototype, the *system* is the computing device platform, and the *components* represent the internal hardware such as motherboard, hard drive, and memory.

In our project description [1], we described an Asset Discovery and Management System as a capability that helps organizations ensure that critical assets (systems) are uniquely identified using known identifiers and device attributes. This capability could include discovery tools that identify endpoints and interrogate the platform for device attributes. However, this prototype demonstration uses alternative platforms for these functions.

4.2.1.1 RSA Archer Governance, Risk, and Compliance (GRC) Platform

The RSA Archer GRC Platform supports business-level management of governance, risk, and compliance programs. The GRC Platform serves as the foundation for all RSA Archer solutions and allows an organization to adapt the solutions to business requirements, build their own applications, and integrate with other external data sources. This prototype demonstration incorporates an Archer use case centered on asset management and continuous monitoring.

RSA Archer is a web-based platform that operates on a Microsoft stack consisting of Windows Server, Internet Information Services, and SQL Server. This prototype demonstration leverages the RSA Archer Data Feed Manager capability that allows consumption of external data via delimited text files, Extensible Markup Language (XML) or JavaScript Object Notation (JSON) data on network locations, File Transfer Protocol (FTP), or Hypertext Transfer Protocol (HTTP) or HTTP Secure (HTTPS) sites. As of this publication, the demonstration imports JSON enterprise asset data and platform integrity data via the HTTPS Data Feed Manager.

Additionally, the RSA Archer Platform solution has a number of built-in applications which assist organizations with risk management by way of business processes and workflows. In this prototype

588 demonstration, we leverage a customized version of the Devices application which serves as a central
589 repository for knowledge, such as platform attributes and other manufacturing information, about
590 computing devices within an organization.

591 The default Devices application enables an organization to manage IT assets, such as computing devices,
592 to ensure that they are protected according to management expectations. Within the scope of this
593 demonstration, the Devices application provides a holistic continuous monitoring platform that allows IT
594 administrators to ensure computing devices within their organization have not been tampered with or
595 otherwise modified. To augment the Devices application, this demonstration has created an additional
596 custom application named Components that stores component information associated with each
597 computing device.

598 Finally, we modeled the structure of the Components application and made customizations to the
599 Devices application via data fields to mimic the structure of the TCG Platform Certificate Profile as a
600 vendor-agnostic method of storing data such as manufacturer, model, and version information. For
601 organizations using the broader Archer GRC platform capabilities, such as third-party risk management,
602 records (computing devices) stored in the Devices application can also be associated with other aspects
603 of the enterprise infrastructure [9].

604 The computing device data described above are consolidated and made available to an IT administrator
605 via an information management console or "dashboard" which also incorporates operational continuous
606 monitoring aspects described from Scenario 3. A *dashboard* in the context of this prototype is a tool that
607 consolidates and communicates information relevant to the organizational security posture in near real-
608 time to security management stakeholders [7].

609 4.2.2 Configuration Management System

610 The focus of this document is on implementing the information system security aspects of configuration
611 management, and as such the term security-focused configuration management (SecCM) is used to
612 emphasize the concentration on information security. The goal of SecCM activities is to manage and
613 monitor the configurations of information systems to achieve adequate security and minimize
614 organizational risk while supporting the desired business functionality and services [7].

615 As defined in the project description [1], a configuration management system is a component that
616 enforces corporate governance and policies through actions such as applying software patches and
617 updates, removing denylisted software, and automatically updating configurations. These components
618 may also assist in management and remediation of firmware vulnerabilities.

619 SP 800-128 [7] further defines two fundamental concepts that this prototype demonstration references:
620 baseline configuration and configuration monitoring.

621 A *baseline configuration* is a set of specifications for a system, or configuration items within a system,
622 that has been formally reviewed and agreed on at a given point in time, and which can be changed only

through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes. In the context of this prototype demonstration, the baseline configuration represents the platform attributes (e.g., serial number, embedded components, firmware and software information, platform configuration) asserted in the OEM's verifiable artifact. The baseline configuration may be updated if a configuration change (e.g., adding hardware components, updating firmware) is approved by an organization's change management process.

Configuration monitoring is the process for assessing or testing the level of compliance with the established baseline configuration and mechanisms for reporting on the configuration status of items placed under configuration management. This prototype demonstration uses a combination of monitoring capabilities provided by the configuration management system and OEM platform validation tooling to assess whether the computing device has deviated from the defined baseline configuration.

4.2.2.1 Microsoft Endpoint Configuration Manager

Many organizations may already use Microsoft Endpoint Configuration Manager capabilities such as application management, organizational resource access, and operating system (OS) deployment. This prototype demonstration leverages the existing configuration management activities and extends them to include compliance settings (a set of tools and resources that can help you to assess, track, and remediate the configuration compliance of client devices in the enterprise) and reporting (a set of tools and resources that help you use the advanced reporting capabilities of SQL Server Reporting Services from the Configuration Manager console [10]). These capabilities align to the SP 800-128 best practice of using automation, where possible, to enable interoperability of tools and uniformity of baseline configurations across the computing device.

The computing device baseline configuration (defined above) was evaluated using the compliance settings capability. In the Intel laptop use case, we defined a configuration item which deployed a custom PowerShell script to each Intel computing device. The script executed the `TSCVerifyUtil` tool that is part of the Intel Transparent Supply Chain platform to perform two tests:

- a comparison of scanned components to the OEM-generated platform manifest, and
- validation of the platform certificate bound to the computing device.

If either of the tests fail, an error code is returned to Configuration Manager, where an IT administrator could take remediation action.

Similarly, we use a set of PowerShell commands provided by HP Inc., called the Client Management Script Library (CMSL), in a custom script to detect unexpected hardware or component changes. The CMSL incorporates several modules, including two directly related to this demonstration—the BIOS and Device module, and the Firmware module.

Finally, this demonstration leverages an existing Configuration Manager platform by extending its capabilities by way of a console plug-in provided by an OEM, HP Inc.. The plug-in, HP Manageability

Integration Kit (HP MIK), enables an administrator to manage security features that are specific to HP Inc. computing devices.

4.3 Supporting Platform Integrity Validation Systems

This section describes supplemental services and systems that support the security characteristics defined in Section 3.4.3.1. These systems integrate with existing services that an enterprise may already have fielded, as described in Section 4.2.

4.3.1 Host Integrity at Runtime and Start-up Attestation Certificate Authority (HIRS ACA)

The HIRS ACA [11] is described by the project owners, the National Security Agency, as a proof of concept/prototype intended to spur interest and adoption of Trusted Computing Group standards that leverage the TPM. It is intended for testing and development purposes only, such as this prototype demonstration, and is not intended for production environments. The ACA's functionality supports the provisioning of both the TPM 1.2 and TPM 2.0 with an Attestation Identity Credential (AIC); however, in this prototype we have only exercised TPM 2.0 capabilities.

The HIRS ACA includes a flexible validation policy configuration capability, and in this demonstration's defined scenarios, is configured to enforce the Validation of Endorsement and Platform Credentials to illustrate a supply chain validation capability.

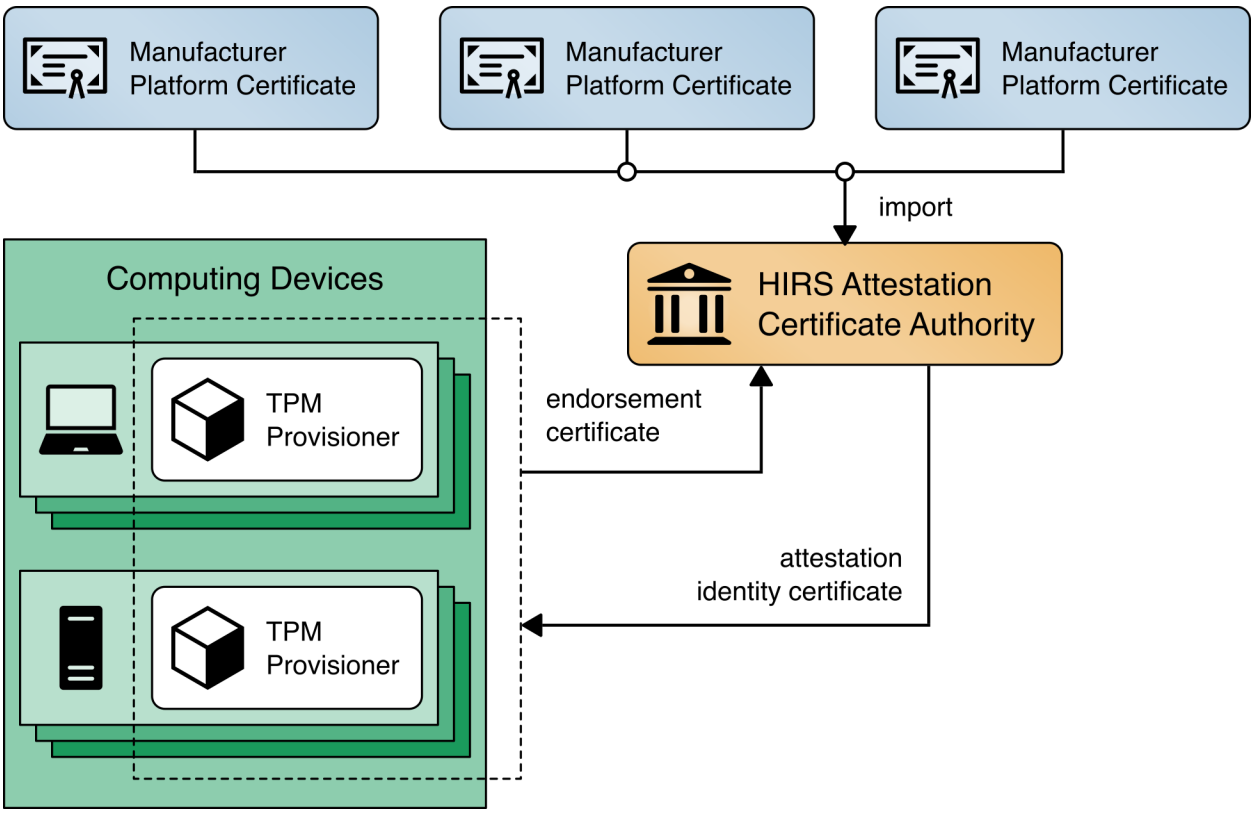
The HIRS ACA project is comprised of multiple components and services that are utilized in this prototype demonstration. The first component, named the TPM Provisioner, is a software utility executed on the target computing device. It takes control of the TPM if it is not already owned and requests an AIC for the TPM from the Attestation Certificate Authority (ACA, described below). The Provisioner communicates with the ACA through a representational state transfer (REST) API interface to complete the transaction. As part of the transaction, the TPM Provisioner reads the Endorsement Key credentials from the TPM's non-volatile random access memory (NvRAM) and interrogates the computing device's hardware, network, firmware, and OS info for platform validation.

The Attestation Certificate Authority (ACA) the server component that issues AICs to validated devices holding a TPM. It performs TCG-based Supply Chain Validation of connecting clients by Validating endorsement and Platform Credentials. The (ACA) is in alignment with the TCG EK Credential Profile For TPM Family 2.0 specification to ensure the endorsement key used by the TPM was placed there by the manufacturer. It also aligns with TCG Platform Attribute Credential Profile Specification Version 1.1 Revision 15 while processing platform credentials to verify the provenance of the system's hardware components, such as the motherboard and chassis, by comparing measured component information against the manufacturers, models, and serial numbers listed in the Platform Credential.

691 Finally, the ACA Dashboard is the Endorsement and Platform Credential policy configuration front end
692 enables the IT Administrator to view all validation reports, credentials, and trust chains. IT
693 Administrators also use this interface to upload, and if necessary, remove, certificate trust chains,
694 Endorsement and Platform credentials.

695 Figure 4-3 HIRS ACA Platform presents a high-level view of how the HIRS system integrates with our
696 prototype demonstration.

697 **Figure 4-3 HIRS ACA Platform**

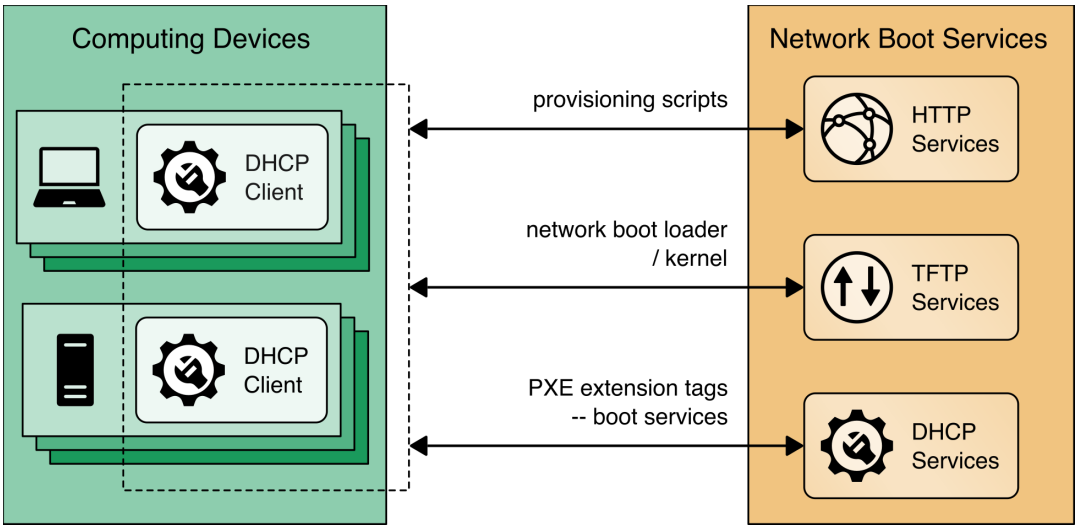


698 4.3.2 Network Boot Services

699 The computing devices in this prototype demonstration support a Dynamic Host Client Protocol (DHCP)
700 based Preboot Execution Environment (PXE), which enables an IT administrator to boot the device over
701 the network. In our environment, the IT administrator can boot into either a customized CentOS7 or a
702 WinPE OS, depending on the platform validation tools that are needed. The CentOS7 environment
703 supports the TPM Provisioner component of the HIRS ACA Platform, the Eclypsium Portable Scanner,
704 and automation scripts. Figure 4-4 details the flow of the boot environment:

1. Computing devices are configured to boot over the network via a network interface card (NIC). The DHCP server presents the boot options to the IT administrator. Once the OS is chosen, the DHCP server directs the DHCP client to the Trivial File Transfer Protocol (TFTP) server.
2. The DHCP client downloads and executes boot loaders and kernels associated with the target OS.
3. (CentOS7 Only) The IT administrator downloads the latest provisioning script from a centralized repository.

Figure 4-4 Network Boot Services Environment



4.3.3 Platform Manifest Correlation System

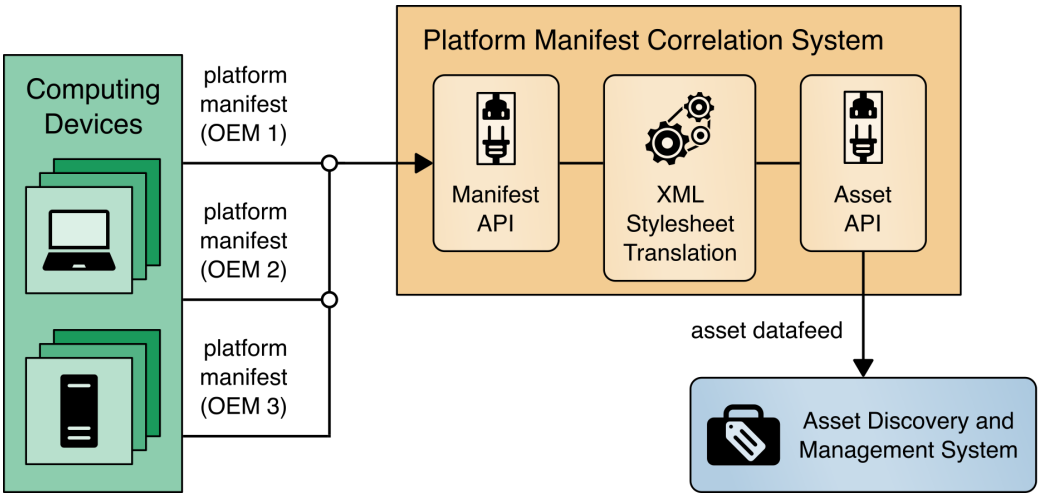
This system assists in providing computing device manifest attributes to the asset management system. The system was built specifically for this demonstration and was built on open-source projects to include the node.js server platform. The requirements of this system were defined as:

1. Provide a web interface for the IT administrator to upload platform manifests.
2. Provide a REST application programming interface (API) for scripts to upload platform manifests.
3. Provide a REST API for the asset management system to periodically poll for new computing devices to import in the repository.

Once the platform manifest is uploaded, it is converted to a common XML format that has been defined within the RSA Archer administration console via an XML Stylesheet Translation (XSLT). During this initial phase of the prototype demonstration, two XSLTs have been defined that support manifests from the HIRS ACA Provisioner and Intel's TSC applications.

Figure 4-5 presents how it is integrated into the larger architecture.

Figure 4-5 Platform Manifest Correlation System

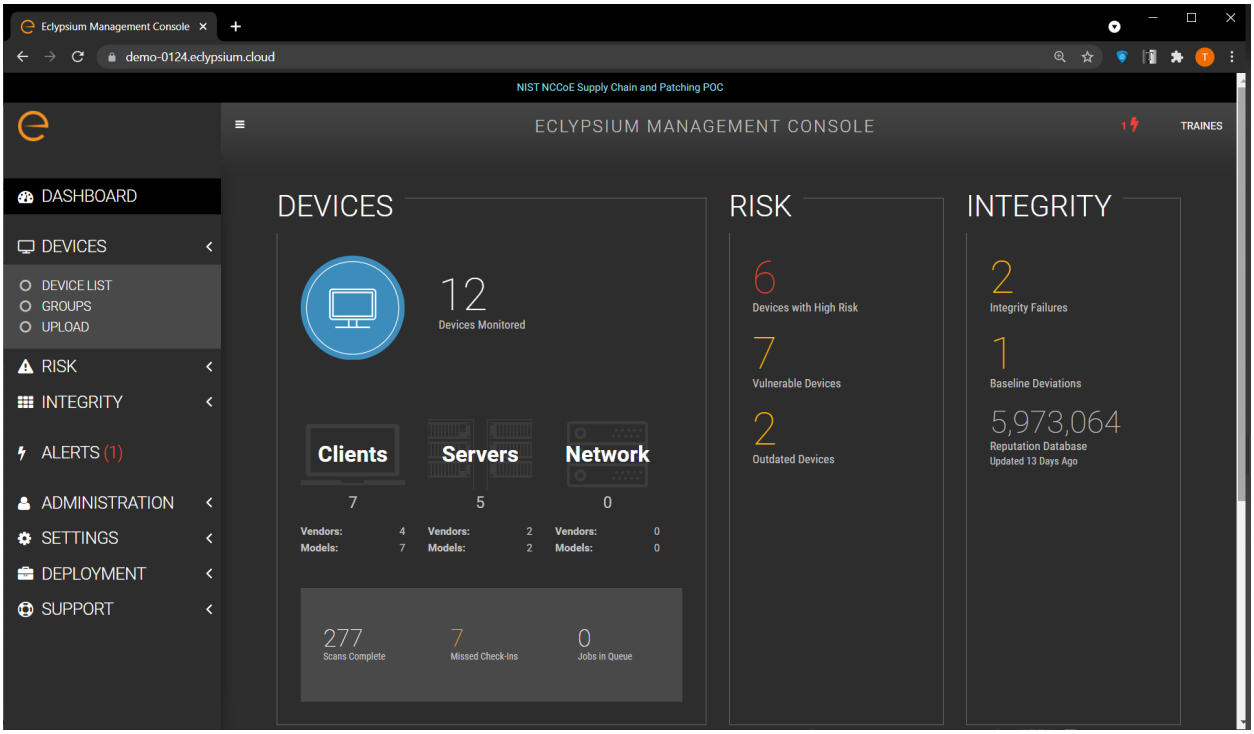


4.3.4 Eclypsium Analytic Platform

The Eclypsium platform is a security solution that focuses on vulnerabilities and threats below the OS layer, to include firmware and component hardware. The platform consists of an endpoint agent, which can be deployed from an enterprise systems configuration manager on each computing device, the analysis backend (either cloud or on-premises), and the device reputation cloud service. The platform continuously updates a profile for each device and collects telemetry about each computing device into the analysis backend. The device reputation cloud provides a database of collected vulnerabilities that could potentially affect computing device components within an organization.

The initial endpoint agent scan of the computing device forms a baseline profile, which is used for later comparisons against the original profile stored in the Analysis Backend. Any deviations from the profile are detected and can be communicated to an organization's IT Security department as an integrity issue in multiple ways according to organization policy. For example, the IT Security department can be alerted when the system firmware version has changed from the baseline, which could indicate an unexpected firmware swap or tampering of the computing device in the operational environment. This prototype demonstration leverages a combination of Eclypsium's REST API (Scenario 3 – operational monitoring) and web-based dashboard captured in Figure 4-6 (Scenario 2 – provisioning of the computing device).

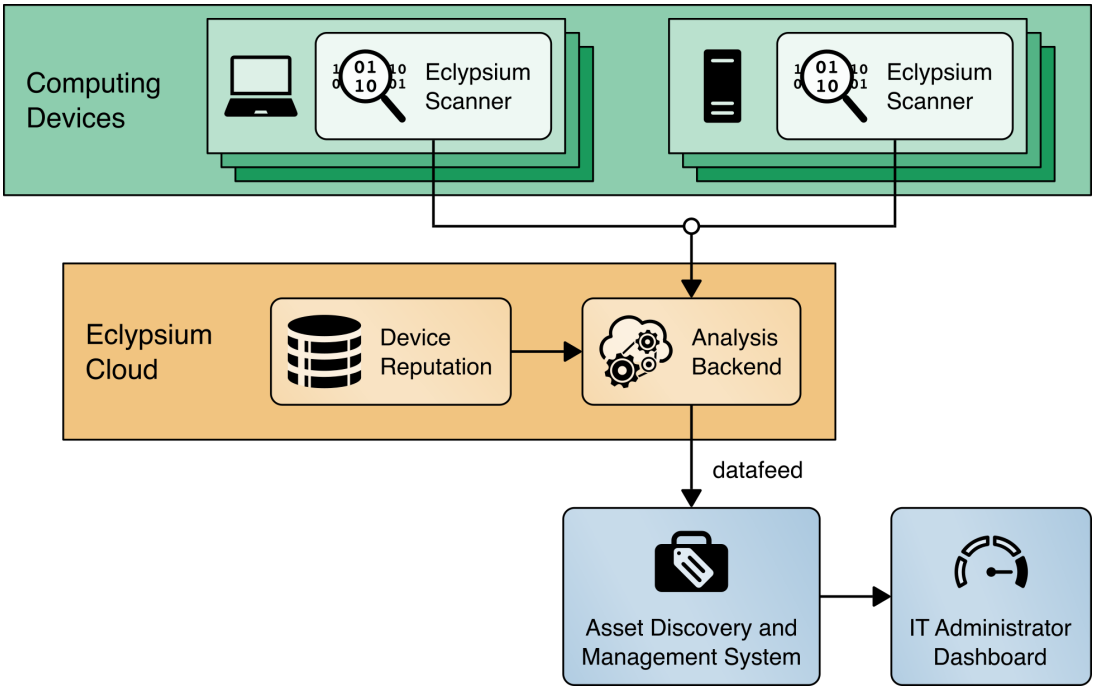
744 **Figure 4-6 Eclypsium Management Console**



745 In Scenario 2, this demonstration uses a portable version of the Eclypsium agent, as opposed to the
746 installer-based version used in Scenario 3. This is to support an ephemeral environment for the IT
747 administrator where computing device acceptance testing is performed. We have integrated this
748 portable version of the agent into the CentOS7 discussed in Section 4.3.2.

749 Figure 4-7 presents how this project integrates Eclypsium's cloud services into the architecture.

750 **Figure 4-7 Eclypsium Analytics Platform**



751 ## 4.4 Computing Devices

752 In this prototype demonstration we define a computing device as client and server devices associated
753 with verifiable artifacts. These devices may contain several integrated platform components or
754 subsystems from multiple manufacturers. Our manufacturing partners, HP Inc., Dell Technologies,
755 Hewlett Packard Enterprise, Seagate, and Intel have contributed hardware to the project.

756 ### 4.4.1 HP Inc.

757 HP Inc. functions as an OEM within this prototype demonstration and contributed two HP Inc. Elitebook
758 360 830 G5 laptops. Each laptop has a TCG-Certified TPM v2.0 with embedded EK Certificate.

759 In support of Scenario 1, the NCCoE lab is utilizing the HIRS Platform Attribute Certificate Creator
760 (PACCOR) project to generate a representative Platform Certificate bound to the device identity. The
761 Platform Certificate was signed by HP Inc.'s internal test certificate authority.

762 In support of Scenario 2, acceptance testing of the HP Inc. laptops is performed via the HIRS ACA TPM
763 Provisioner described in Section 4.3.1.

764 In support of Scenario 3, the demonstration will utilize a combination of Microsoft Endpoint
765 Configuration Manager integrated with the HP MIK and HP Client Management Script Library (CMSL)

PowerShell scripting library for enterprise manageability of platform hardware and firmware security capabilities (e.g., firmware integrity breach detection and physical tampering detection). As described in Section 4.2.2.1, this demonstration makes use of HP Inc's CMSL PowerShell modules. Specifically, the BIOS and Device module provides basic querying of device attributes and secure manipulation of HP BIOS settings and managing the HP BIOS, while the Firmware module provides functionality for interfacing with the HP BIOS firmware, such as gathering security-related events from the HP Endpoint Security Controller hardware.

Finally, this demonstration utilizes HP Inc. capabilities that augment tooling used to verify the integrity of computing device components during use. These capabilities are intended to be provisioned during the computing device acceptance testing process before issuance to the end user for operational use, and can optionally be provisioned in manufacturing and included in the device acceptance testing process.

- **HP Secure Platform Management** enforces a certificate-based authorization model that enables firmware setting security management by an IT administrator. The model is composed of two keys, an Endorsement Key and a Signing Key (note: the Endorsement Key in this context is not related to the TPM Endorsement Key). The Endorsement Key's primary purpose is to protect against unauthorized changes to the Signing Key. The Signing Key is used by the platform to authorize commands sent to the firmware (BIOS) [12] [13].
- **HP Sure Start** is a built-in hardware security system that protects platform firmware code and data (including HP BIOS, HP Endpoint Security Controller firmware, and Intel Management Engine firmware) from accidental or malicious corruption by (1) detecting corruption and then (2) automatically restoring the firmware to its last installed HP-certified version and the data (settings) to the last authorized state. The capability also stores events related to firmware integrity that can provide visibility into attempted firmware integrity breaches [14].
- **HP Sure Recover** is an OS recovery mechanism that is completely self-contained within the hardware and firmware to allow secure OS recovery from the network or from a local OS recovery copy stored in dedicated flash on the system board. It includes settings that control when, how, and from where BIOS installs the OS recovery image, and which public keys are used by BIOS to validate the integrity of the recovery image. It can also record events due to OS recovery image integrity failures [14].
- **HP TamperLock** provides a general protection mechanism against all classes of physical attacks that involve removal of the system cover to obtain access to the system board. This is achieved by providing a cover removal sensor to detect and lock down a system that is disassembled, along with fully manageable policy controls to configure what action to take in the event a cover removal is detected. Cover removal events and history are stored in platform hardware and can be queried by a remote administrator [15].
- The **HP Endpoint Security Controller** is HP's hardware root of trust that enables all the features above and provides isolated/dedicated non-volatile storage on the system board that (1)

enables recovery of firmware code and data, policies, and OS images, as well as (2) secure hardware-based storage for tampering-related events associated with each of the capabilities described above.

4.4.2 Dell Technologies

Dell contributed hardware and supporting software as part of a pilot program that are aligned with the defined security characteristics of this prototype demonstration.

The demonstration uses two Dell Precision 3530 laptops as the client computing devices that are evaluated through an enterprise acceptance testing process. These computing devices are equipped with a TPM that is compatible with the TCG's 2.0 specification as discussed in Section 3.6.1. In alignment with the TCG specifications, the TPM endorsement keys were generated by Nuvoton, a supplier of TPMs to OEMs.

In support of Scenario 1, Dell supplied the NCCoE with the infrastructure and tooling to support TCG Platform Certificate generation during Dell computing device manufacturing. Once executed, the tooling collected the computing devices component data and created a Platform Certificate. The Platform Certificate was bound to the device identity (TPM) and digitally signed by a Dell factory Hardware Security Module. The Platform Certificate was stored within the Extensible Firmware Interface (EFI) system partition, where it was later extracted for use in supporting platform integrity validation systems.

In support of Scenario 2, the validation of component authenticity during acceptance testing of the Dell laptops was performed via the HIRS ACA TPM Provisioner described in Section 4.3.1.

4.4.3 Intel

Intel contributed hardware, supporting software, and cloud services that are aligned with the defined security characteristics of this prototype demonstration through its Transparent Supply Chain platform, or TSC [15] *HP TamperLock: Protecting Devices from Physical Attacks*, HP Inc, 2021, 6 pp. Available: https://www8.hp.com/h20195/v2/GetPDF.aspx/4AA7-8167ENW.pdf.

[16]. TSC enables organizations to verify the authenticity and firmware version of systems and their components. The remainder of this section summarizes the TSC components used within this prototype demonstration; however, it is not an exhaustive description of the complete platform. Refer to Intel's TSC website for complete documentation.

The process starts at the OEM, where an Intel-provided tool called `TSCMFGUtil` enables the creation of a platform certificate data file that is compliant with the TCG Platform Certificate Profile Specification Version 1.1. The `TSCMFGUtil` also generates the Direct Platform Data (DPD) file capturing the Platform Snapshot before shipping the platform out to the customer. The platform certificate data file contains TPM information such as the Platform Configuration Registers (PCRs), the TPM Serial Number, and the

TPM Endorsement Key. The DPD file contains information about the components within the computing device such as component manufacturer part number, batch number, and serial and lot number, as well as sourcing information. The OEM then uploads these files to Intel's Secure File Transport Protocol (SFTP) site where they are processed and digitally signed.

Next, after the computing device is purchased by an organization's IT department, an administrator downloads the DPD file and Platform Certificate from the Transparent Supply Chain Web Portal as part of the computing device acceptance testing process. The aforementioned files are processed by Intel software intended for the end customer, the `AutoVerifyTool`. In this prototype demonstration, the `AutoVerifyTool` enables the following capabilities for the IT administrator:

1. The `ScanSystem` function initiates the scanning of the system components and the TPM information. The scanning operation will perform the following operations:
    a. Read the following platform components: BIOS, system, motherboard, chassis, processor, dual in-line memory modules (DIMMs), batteries, Intel Active Management Technology firmware version, power supplies
    b. Read the TPM PCRs, public Endorsement Key, and the Endorsement Key serial number
    c. Read the internal drive information
    d. Read the Windows Management Instrumentation (WMI) Information for internal keyboard, pointer, and network devices
2. After the system has been scanned, the IT administrator executes the `Read Direct Platform Data File` function which opens and displays the DPD associated with the platform.
3. The IT administrator executes the `Compare` function, which compares the current system component value information that was captured by `ScanSystem` operation to the component value information that was read in from the DPD file.
4. The IT administrator executes the `Platform Certificate Verify` function, which validates the Platform Certificate issued for the platform using the TPM as the hardware root of trust. The `Platform Certificate Verify` will check that the TPM Endorsement Key serial number matches the Endorsement Key serial number in the Platform Certificate. The function will also check that the manufacturer, version, and serial number match the values in the Platform Certificate.

To demonstrate the TSC platform, Intel contributed laptop computing devices from OEMs Lenovo and HP Inc. (T490 Thinkpad and HP EliteBook x360 830 G5, respectively). Intel also provisioned accounts for the NCCoE project team to use the TSC Web Portal for demonstrating computing device acceptance testing described in Scenario 2.

5 Security Characteristic Analysis

The purpose of the security characteristic analysis is to understand the extent to which the project meets its objective of creating a prototype that demonstrates how organizations can verify that the components of their acquired computing devices are genuine and have not been tampered with or otherwise modified throughout the devices' life cycles. In addition, it seeks to understand the security benefits and drawbacks of the prototype solution.

5.1 Assumptions and Limitations

The security characteristic analysis has the following limitations:

- It is neither a comprehensive test of all security components nor a red-team exercise.
- It cannot identify all weaknesses.
- It does not include the lab infrastructure. It is assumed that devices are hardened. Testing these devices would reveal only weaknesses in implementation that would not be relevant to those adopting this reference architecture.
- It will evolve and expand as the project as collaborators are integrated into the final architecture in the next publication of this document.
- Because this is a preliminary draft, testing the prototype implementation is not complete. The content provided in this section is preliminary and incomplete.

5.2 Build Testing

This section addresses how this prototype demonstration addresses each scenario and identifies gaps that will be addressed as the project progresses.

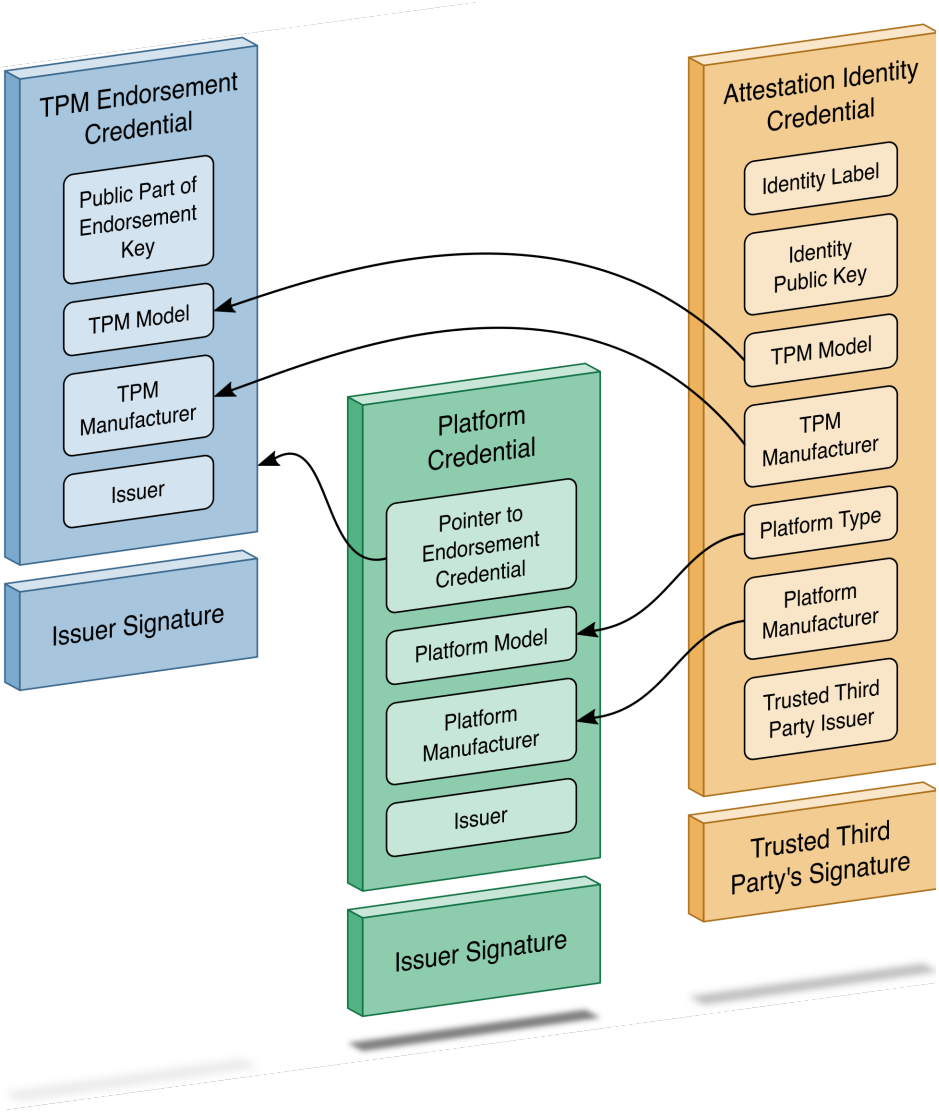
5.2.1 Scenario 1

The desired outcome of Scenario 1 is the creation of verifiable platform artifacts, either by the manufacturer or the customer in the field. This demonstration uses a manufacturer-created platform artifact by way of Intel's Transparent Supply Chain platform. We also emulated a customer-created platform artifact using the HIRS ACA project's Platform Attribute Certificate Creator (PACCOR) software for Dell and HP Inc. laptops. In each case, the platform artifact is signed by a cryptographic key designated only for test/lab purposes. Additionally, the IT administrator uploads the verifiable artifact to the HIRS ACA validation system for use in Scenarios 2 and 3.

In all cases, the platform artifact is instantiated as a Platform Attribute Certificate defined in the TCG Platform Attribute Credential Profile Specification version 1.0. The profile defines structures that extend the X.509 certificate definitions to achieve interoperability between platform validation systems that

902 ingest artifacts. Figure 5-1 shows the relationship between the platform certificate and the TPM
903 Endorsement Credential, based on a graphic from the *TCG Credential Profiles for TPM* [17].

904 **Figure 5-1 Platform Certificate Binding to Endorsement Credential**



905 We use an open-source tool (openssl) to parse one of our demonstration platform artifacts to validate
906 alignment with the TCG specification. Note that the current profile allows the manufacturer to choose
907 between Attribute Certificate or Public Key Certificate format. The example in Table 5-1 uses the
908 Attribute Certificate format and is not an exhaustive comparison of all requirements within the profile. It
909 is intended to highlight the binding of authoritative attributes (Attribute Extension) to the hardware
910 itself (Holder).

911 **Table 5-1 Prototype Platform Artifact**

Platform Certificate Assertion	Field Name	Field Description
SEQUENCE SET SEQUENCE OBJECT :countryName PRINTABLESTRING :US SET SEQUENCE OBJECT :stateOrProvinceName UTF8STRING :California SET SEQUENCE OBJECT :localityName UTF8STRING :Palo Alto SET SEQUENCE OBJECT :organizationName UTF8STRING :HP Inc. SET SEQUENCE OBJECT :organizationalUnitName UTF8STRING :HP Labs Pilot SET SEQUENCE OBJECT :commonName UTF8STRING :HP Inc. CIV-NCCOE-Test	Issuer	Distinguished name of the platform certificate issuer
SEQUENCE SET SEQUENCE OBJECT :countryName PRINTABLESTRING :DE SET SEQUENCE OBJECT :organizationName UTF8STRING :Infineon Technologies AG SET SEQUENCE OBJECT :organizationalUnitName UTF8STRING :OPTIGA(TM) SET SEQUENCE OBJECT :commonName	Holder	Identity of the associated TPM EK Certificate

Platform Certificate Assertion	Field Name	Field Description
UTF8STRING :Infineon OPTIGA(TM) TPM 2.0 RSA CA 042		
SEQUENCE OBJECT :2.23.133.18.3.1 OCTET STRING 00020001 UTF8STRING :HP UTF8STRING :10	Attribute Extension	Example Component Class of type Chassis

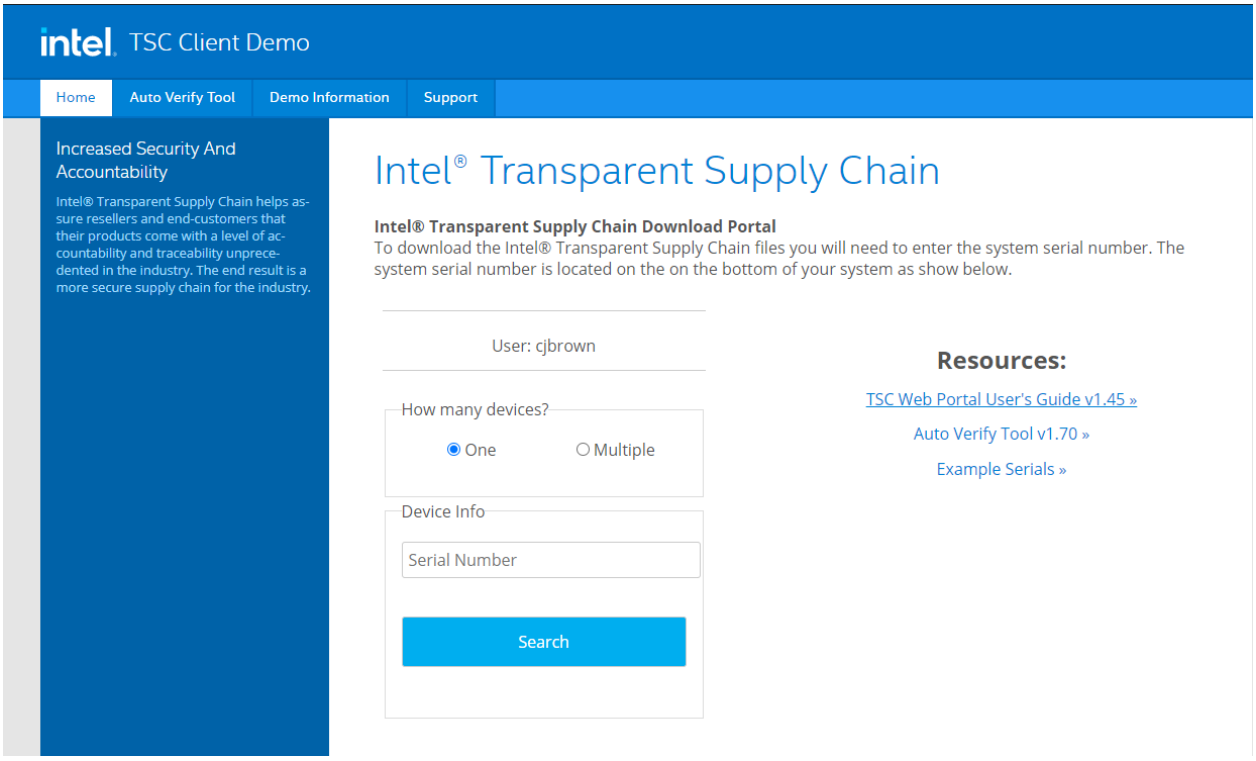
5.2.2 Scenario 2

The desired outcome of Scenario 2 is to verify the provenance and authenticity of a computing device that has been received through non-verifiable channels. The project description defined four notional steps that an IT administrator might perform to augment, not replace, an existing asset management acceptance testing process. The remainder of this section discusses the status of each step, with supplemental sequence diagrams available in Appendix C.

Step 1: As part of the acceptance testing process, the IT administrator uses tools to extract or obtain the verifiable platform artifact associated with the computing device.

Using the Intel Transparent Supply Chain platform, an IT administrator obtains the verifiable artifact from the download portal in two ways—manually via the web interface, and programmatically through the download portal API, depending on the organizational use case. Currently, we demonstrate the manual process where an IT administrator uses a web browser to access the Intel download portal, input the computing device serial number, and download the associated verifiable artifacts. The download portal API may be useful for organizations that have an automated computing device acceptance testing process. The download portal screenshot in Figure 5-2 provides a visual of the interface viewed from the IT administrator's perspective.

928 **Figure 5-2 Intel Transparent Supply Chain Download Portal**



929 In this prototype demonstration for the Dell and HP Inc platforms, the IT administrator obtains the
930 platform verifiable artifact from the EFI system partition storage (ESP). The ESP provides a convenient
931 storage mechanism because it is available by all manufacturers that support Unified Extensible Firmware
932 Interface (UEFI) and is OS-independent. Therefore, it is accessible either through our Linux network boot
933 environment or through the native OS (Windows 10). Alternatively, the verifiable artifact can be
934 delivered to the IT administrator through an out-of-band process or stored directly on the TPM, if
935 available on the computing device.

936 **Step 2:** The IT administrator verifies the provenance of the device's hardware components by validating
937 the source and authenticity of the artifact.

938 **Step 3:** The IT administrator validates the verifiable artifact by interrogating the device to obtain
939 platform attributes that can be compared against those listed in the artifact.

940 For simplicity, we have combined discussion of steps 2 and 3 because they are performed in tandem
941 using platform validation tools.

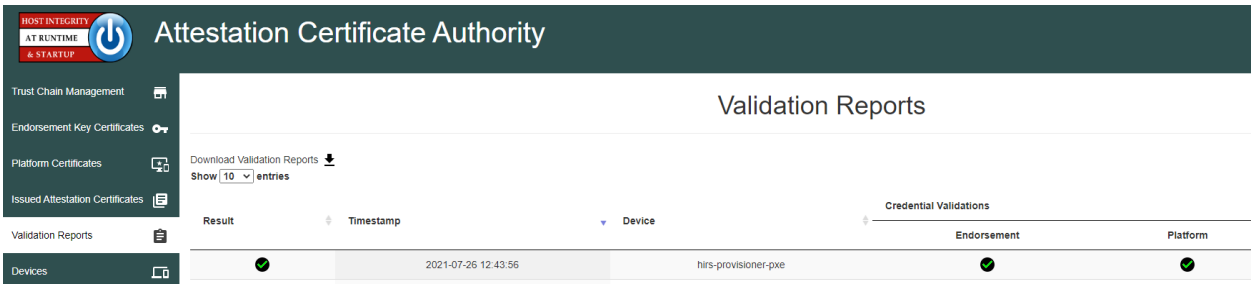
942 In the Intel TSC platform, we execute the `AutoVerifyTool` described in Section 4.4.2 to verify the
943 provenance of the device's hardware components in the native Windows 10 environment using the

verifiable artifact retrieved from Step 1. The tool is pre-configured with trusted manufacturer signing certificates that are used in the validation process. Second, the IT administrator scans the machine using the `AutoVerifyTool`, where the results are compared against those listed in the artifact. The tool subsequently gives the IT administrator a visual indicator of whether or not the validation process was successful. The tool can be accessible to the IT administrator in a number of ways, depending on the existing acceptance testing process. For this prototype, the tool is available to the IT administrator via a network share accessible to IT staff with sufficient privileges.

In this prototype demonstration for the Dell and HP Inc platforms, prior to the acceptance testing process, the IT administrator supplies the verifiable artifact's (platform certificate's) root (and potentially intermediate) Certificate Authority (CA) certificates to the HIRS ACA portal to form a chain used later in the validation process. This process is repeated for the endorsement credential issuing certificates. We recommend that readers of this guide contact their specific manufacturer to retrieve the correct certificate chain to reduce the risk of validation failures.

Next, the IT administrator boots the target computing device into the ephemeral Linux CentOS7 environment described in Section 4.3.2 where the HIRS ACA Provisioner component is installed. Here, the IT administrator runs a script where the Provisioner is invoked, and the provenance of the device's hardware components is verified by the HIRS ACA backend component. The IT administrator confirms validation of the verifiable artifact by observing the output of the script and optionally accessing the HIRS ACA portal web interface, as shown in Figure 5-3. The checkmark in the Result column indicates the verifiable artifact has been validated and the assertions made by the artifact have been validated against the interrogation process.

Figure 5-3 HIRS ACA Validation Dashboard



Finally, in addition to the platform validation steps described above, this prototype demonstration interrogates and analyzes the target computing device across all participating manufacturers using the Eclypsium platform described in Section 4.3.4. This analysis gives the IT administrator immediate feedback to any firmware integrity issues, such as an unexpected or outdated firmware version, and can be corrected before being fielded to the end user.

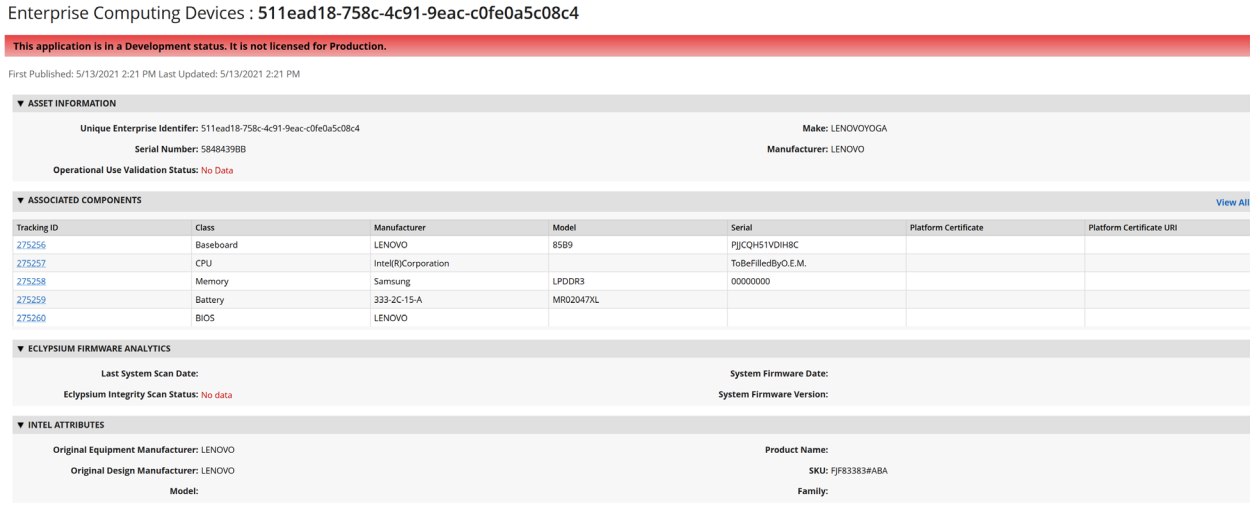
Step 4: The computing device is provisioned into the Asset Discovery and Management System and is associated with a unique enterprise identifier. If the administrator updates the configuration of the

platform (e.g., adding hardware components, updating firmware), then the administrator might create new platform artifacts to establish a new baseline.

Following the successful platform validation of the target computing device, it is provisioned into the Asset Discovery and Management System described in Section 4.2.1. This demonstration associates the system's Universally Unique Identifier (UUID), available via the System Management BIOS (SMBIOS), with the computing device in the asset management system. The SMBIOS is a standard for delivering management information via system firmware developed by the DMTF (formerly known as the Distributed Management Task Force). The standard presentation format of the SMBIOS provides a benefit to this prototype in that it is available in an OS-independent manner, and therefore available whether using the native Windows 10 environment or our CentOS7 network boot environment. We also associate the system UUID with each computing device that has been provisioned into the Eclypsium platform. This enables the Asset Discovery and Management System to correlate device data from the Eclypsium cloud to existing assets. Organizations that adopt the UUID model described here can extend it to other data sources that store device platform data, provided that the Asset Discovery and Management System is configured to update existing records based on the UUID, and the platform data is mapped to the appropriate data fields in the Asset Discovery and Management System.

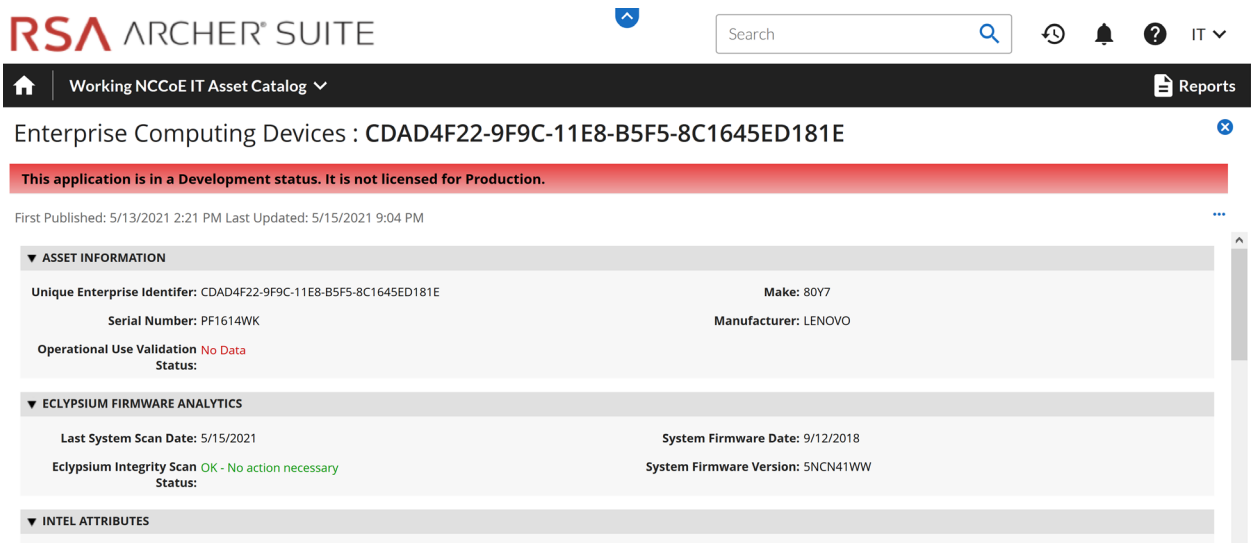
The provisioning process for laptops in this prototype demonstration that are included in the Intel TSC platform uses `TSCVerifyUtil` (Section 4.4.3) to export a platform manifest that is uploaded to the Platform Manifest Correlation System's web-based interface (Section 4.3.3) by the IT administrator. For laptops that use the HIRS ACA platform, we opted to use a script-based approach to automatically upload the platform manifest to the Platform Manifest Correlation System's REST API. This demonstrates flexibility in the architecture that can assist organizations with a heterogeneous manufacturer environment or use cases where automation is not feasible. Figure 5-4 presents an example for an individual computing device that has been provisioned using the Intel TSC platform.

997 **Figure 5-4 Asset Inventory and Discovery Example 1**



998 Once the RSA Archer's JavaScript DataFeed that retrieves data from the Eclypsium cloud runs, the asset
999 record is updated accordingly with system firmware data, as Figure 5-5 shows.

1000 **Figure 5-5 Asset Inventory and Discovery Example 2**



1001 As noted in Section 4.2.1.1, we leverage RSA Archer's JavaScript DataFeed capability to import device,
1002 firmware, and associated component data into the asset repository. The DataFeed can be thought of as
1003 a scheduled job which continuously polls the Platform Manifest Correlation System for new assets. It
1004 also supports updating existing assets in the following ways:

- Two DataFeeds are configured that make REST API transactions with the Eclypsium Analytic Platform. One polls the service for any platform integrity issues that are present on computing devices and the other gathers basic information about installed system firmware, such as the version and date it was published.
- A third DataFeed is configured to make a Structured Query Language (SQL) transaction with the database that supports the Microsoft Endpoint Configuration Manager. Computing devices with unapproved component swaps are reported and consumed by the DataFeed.

Step 4b: A common use case is when the IT administrator replaces a component in a fielded computing device. In this prototype demonstration for systems that use the HIRS ACA platform, the verifiable artifact (platform certificate) is re-generated and uploaded to the HIRS ACA backend, and the device is re-provisioned by the IT administrator. However, for systems that use Intel's TSC platform, the IT administrator uploads the new computing device configuration to the TSC Web Portal using Intel's software tools. The Intel TSC platform subsequently regenerates the verifiable artifacts, and the IT administrator makes them available for download when the provisioning process is restarted. We were able to exercise this process successfully using Intel-contributed laptops.

5.2.3 Scenario 3

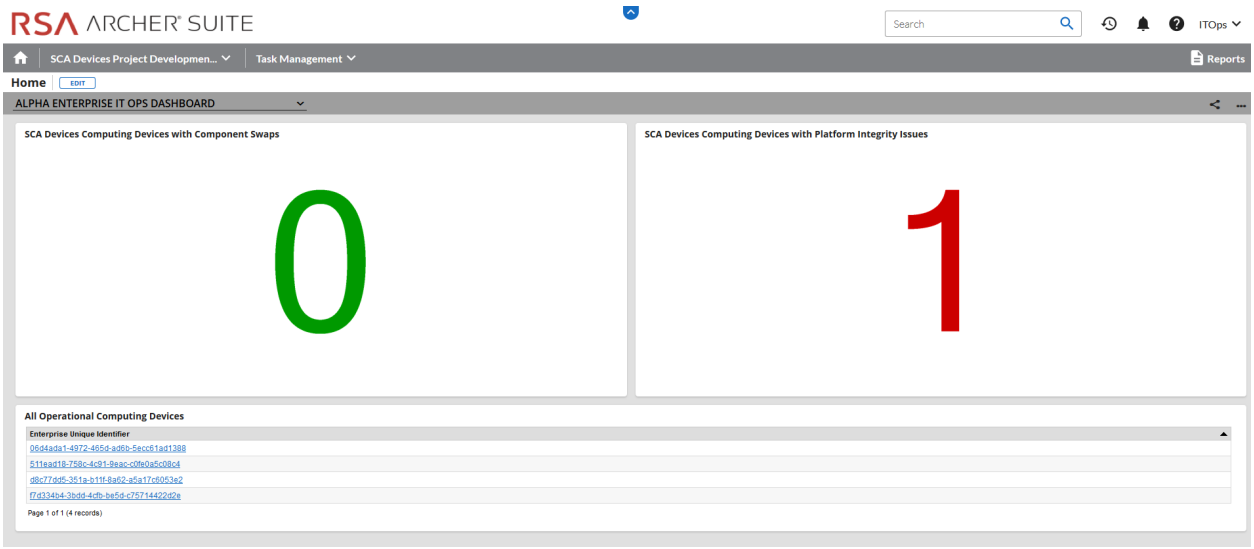
The desired outcome of Scenario 3 is to ensure computing device components are verified against the attributes and measurements declared by the manufacturer or purchasing organization during operational usage. This scenario is primarily enabled by the Configuration Management System (Section 4.2.2). Supplemental sequence diagrams are available in Appendix C.

To support build testing of Intel TSC platforms in this scenario, we used the DPD intended for another system in place of the correct DPD to ensure the Intel platform validation would fail. We repeated this test with an incorrect platform certificate, which also failed validation as expected. Future iterations of this prototype demonstration build testing may expand to include actual hardware component swaps to emulate an operational usage scenario.

A second use case we examined is when system firmware is updated on the fielded laptop. This may be initiated by the end user who is guided by a helpdesk or by the IT administrator. In either case, the Eclypsium scanner that is installed during Scenario 2 detects this change and reflects it in the Eclypsium cloud. The RSA Archer JavaScript DataFeed subsequently ingests the change, and it is reflected in the asset repository.

With the platform and monitoring data collected from scenarios 2 and 3, we created a dashboard pictured in Figure 5-6 that enables the IT Administrator to achieve better visibility into supply chain attacks and detect advanced persistent threats and other advanced attacks.

1038 **Figure 5-6 Scenario 3 Dashboard**



1039 5.3 Scenarios and Findings

1040 One aspect of our security evaluation involved assessing how well the reference design addresses the
1041 security characteristics that it was intended to support. The Cybersecurity Framework Subcategories
1042 were used to provide structure to the security assessment by consulting the specific sections of each
1043 standard that are cited in reference to a Subcategory. The cited sections provide validation points that
1044 the example solution would be expected to exhibit. Using the Cybersecurity Framework Subcategories
1045 as a basis for organizing our analysis allowed us to systematically consider how well the reference design
1046 supports the intended security characteristics.

1047 5.3.1 Supply Chain Risk Management (ID.SC)

1048 *5.3.1.1 ID.SC-4: Suppliers and third-party partners are routinely assessed using audits,*
1049 *test results, or other forms of evaluations, to confirm they are meeting their*
1050 *contractual obligations.*

1051 This Cybersecurity Framework Subcategory is supported in the prototype implementation by the Intel
1052 TSC and the HIRS ACA platforms. Specifically, Scenario 2 acceptance testing acts as an initial evaluation
1053 of the manufacturer (supplier) to validate the source and integrity of assembled components for the
1054 recipient organization of the computing device.

5.3.2 Asset Management (ID.AM)

5.3.2.1 ID.AM-1: Physical devices and systems within the organization are inventoried

This Cybersecurity Framework Subcategory is supported in the prototype implementation by RSA Archer and the Platform Manifest Correlation System. When used in conjunction, they form the basis of an Asset Discovery and Management System that accurately reflects computing devices within an organization, including all components therein.

5.3.3 Identity Management, Authentication and Access Control (PR.AC)

5.3.3.1 PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions

This Cybersecurity Framework Subcategory is supported in the prototype implementation by RSA Archer, Intel, HP Inc, and Dell. The manufacturers in this prototype support device-unique identifiers which are associated with organizational computing devices. Identifiers are prevented from being re-used through RSA Archer policy constraints.

5.3.4 Data Security (PR.DS)

5.3.4.1 PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity

This Cybersecurity Framework Subcategory is supported in the prototype implementation by the Intel TSC platform, Eclypsium, and the HIRS ACA platform. Together, they provide the capability to detect unauthorized changes to firmware. Manufacturers HP Inc and Dell provide capabilities to report firmware version information.

5.3.4.2 PR.DS-8: Integrity-checking mechanisms are used to verify hardware integrity

This Cybersecurity Framework Subcategory is supported in the prototype implementation by RSA Archer and Microsoft Configuration Manager. Together, these products provide the capability to document, manage, and control the integrity of changes to organizational computing devices.

5.3.5 Security Continuous Monitoring (DE.CM)

5.3.5.1 DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed

This Cybersecurity Framework Subcategory is supported in the prototype implementation by RSA Archer, Microsoft Configuration Manager, and Eclypsium. Together, these products form part of an organizational continuous monitoring program. Microsoft Endpoint Configuration Manager and the

Eclypsium platform enable automated monitoring of computing devices for hardware and firmware integrity issues at an organization-defined frequency. This security information is made available to organizational officials through the RSA Archer dashboard, where a risk management decision can be made when a computing device is deemed out of compliance.

6 Future Build Considerations

In this Preliminary Draft, we have described an architecture that decreases the risk of a compromise to products in an organization's supply chain, which in turn may reduce risks to customers and end users that use laptops operationally. The NCCoE recognizes the challenge that organizations face validating the integrity of other computing devices, such as servers. In future iterations of this project, we will incorporate servers into the architecture, to include hardware contributed by Hewlett Packard Enterprise, Intel, Dell, and Seagate. Additional Supporting Platform Integrity Validation Systems may also be added to support the integration of server computing devices.

We also plan to add technical capabilities to the architecture that will further support automation and enhance dashboard visibility for the IT administrator, to include the following:

- Extend the Platform Manifest Correlation System to accept push notifications (via webhooks) from the Eclypsium platform. Additionally, leverage Archer's RESTful APIs to push alerts from the Eclypsium platform and immediately update the compliance dashboard.
- Incorporate manufacturer-specific remediation actions into the dashboard when computing devices are deemed out of compliance.
- Automatically deploy the Eclypsium scanner to computing devices via the Microsoft Configuration Manager while maintaining association with the enterprise unique identifier.
- Expand the dashboard application to include third-party risk management of manufacturers to better understand the risk profile of assets.
- Create a reference implementation that supports the secure creation of cryptographic key pairs that are used in the provisioning and management of HP Inc. hardware. This version of the build will use test key material provided by HP Inc.
- Integrate the configuration baseline status of computing devices with the IT administrator dashboard to detect policy violations as a basis for remediation actions.

Appendix A List of Acronyms

ACA	Attestation Certificate Authority
AIC	Attestation Identity Credential
API	Application Programming Interface
BIOS	Basic Input/Output System
C-SCRM	Cyber Supply Chain Risk Management
CA	Certificate Authority
CMSL	(HP) Client Management Script Library
DHCP	Dynamic Host Client Protocol
DIMM	Dual In-Line Memory Module
DPD	Direct Platform Data
EFI	Extensible Firmware Interface
EK	Endorsement Key
ESP	EFI System Partition Storage
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GIDEP	Government-Industry Data Exchange Program
GRC	Governance, Risk, and Compliance
HIRS	Host Integrity at Runtime and Start-Up
HP MIK	HP Manageability Integration Kit
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communications Technology
IT	Information Technology
JSON	JavaScript Object Notation
NCCoE	National Cybersecurity Center of Excellence
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NvRAM	Non-Volatile Random-Access Memory
OEM	Original Equipment Manufacturer
OS	Operating System
OT	Operational Technology

PACCOR	Platform Attribute Certificate Creator
PCR	Platform Configuration Register
PXE	Preboot Execution Environment
REST	Representational State Transfer
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SecCM	Security-Focused Configuration Management
SFTP	Secure File Transfer Protocol
SMBIOS	System Management BIOS
SP	Special Publication
TCG	Trusted Computing Group
TFTP	Trivial File Transfer Protocol
TPM	Trusted Platform Module
TSC	(Intel) Transparent Supply Chain
UEFI	Unified Extensible Firmware Interface
UUID	Universally Unique Identifier
VAR	Value-Added Reseller
WMI	Windows Management Instrumentation
XML	Extensible Markup Language
XSLT	XML Stylesheet Translation

Appendix B References

[1] T. Diamond et al., *Validating the Integrity of Computing Devices: Supply Chain Assurance*, National Institute of Standards and Technology (NIST), Gaithersburg, Md., March 2020, 14 pp. Available: https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/tpm-sca-project-description-final.pdf.

[2] J. Boyens et al., *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, NIST Special Publication (SP) 800-161, Gaithersburg, Md., April 2015, 282 pp. Available: https://doi.org/10.6028/NIST.SP.800-161

[3] Joint Task Force, *Guide for Conducting Risk Assessments*, NIST SP 800-30 Revision 1, Gaithersburg, Md., September 2012, 95 pp. Available: https://doi.org/10.6028/NIST.SP.800-30r1.

[4] Joint Task Force, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST SP 800-37 Revision 2, Gaithersburg, Md., December 2018, 183 pp. Available: https://doi.org/10.6028/NIST.SP.800-37r2.

[5] *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, NIST, Gaithersburg, Md., April 2018, 55 pp. Available: https://doi.org/10.6028/NIST.CSWP.04162018.

[6] Joint Task Force, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53 Revision 4, Gaithersburg, Md., April 2013, 462 pp. Available: https://doi.org/10.6028/NIST.SP.800-53r4.

[7] A. Johnson et al., *Guide for Security-Focused Configuration Management of Information Systems*, NIST SP 800-128, Gaithersburg, Md., August 2011, 99 pp. Available: https://doi.org/10.6028/NIST.SP.800-128.

[8] *Trusted Platform Module Library Specification, Family "2.0," Level 00, Revision 01.59*, Trusted Computing Group, November 2019. Available: https://trustedcomputinggroup.org/resource/tpm-library-specification/.

[9] *Archer Platform Documentation—Data Governance Design*, RSA. Available: https://community.rsa.com/t5/archer-platform-documentation/data-governance-design/ta-p/556139.

[10] *Introduction to Configuration Manager*, Microsoft, June 2015. Available: https://docs.microsoft.com/en-us/previous-versions/system-center/system-center-2012-R2/gg682140(v=technet.10).

[11] *Host Integrity at Runtime and Start-up (HIRS): Attestation Certificate Authority (ACA) and TPM Provisioning with Trusted Computing-based Supply Chain Validation*, 2020. Available: https://github.com/nsacyber/HIRS/.

[12] *HP Secure Platform Management with the HP Client Management Script Library*, HP Inc. Available: https://developers.hp.com/hp-client-management/blog/hp-secure-platform-management-hp-client-management-script-library.

[13] *Secure BIOS with HP Sure Admin and CMSL*, HP Inc. Available: https://developers.hp.com/hp-client-management/blog/secure-bios-hp-sure-admin-and-cmsl-upd-292021

[14] *HP Sure Start Whitepaper: Firmware Security and Resilience*, HP Inc, 2021, 24 pp. Available: https://www8.hp.com/h20195/v2/getpdf.aspx/4AA7-6645ENW.pdf.

[15] *HP TamperLock: Protecting Devices from Physical Attacks*, HP Inc, 2021, 6 pp. Available: https://www8.hp.com/h20195/v2/GetPDF.aspx/4AA7-8167ENW.pdf.

[16] *Transparent Supply Chain*, Intel. Available: https://www.intel.com/content/www/us/en/products/docs/servers/transparent-supply-chain.html.

[17] *TCG Credential Profiles For TPM Family 1.2; Level 2*, Specification Version 1.2, Revision 8, Trusted Computing Group (TCG), 2013, 64 pp. Available: https://trustedcomputinggroup.org/wp-content/uploads/Credential_Profiles_V1.2_Level2_Revision8.pdf

Appendix C Project Scenario Sequence Diagrams

Figure 6-1 and Figure 6-2 illustrate the flow of interactions between Dell laptops and supporting software that achieves the security characteristics of Scenario 2. Similarly, Figure 6-3 and Figure 6-4 illustrate the interactions between the Intel TSC software tooling and the laptops contributed by Intel for Scenario 2, while Figure 6-5 details Scenario 3. We have represented the client components that are installed on the computing device and the server components as boxes across the top.

Figure 6-1 Dell Laptop Scenario 2 Part 1

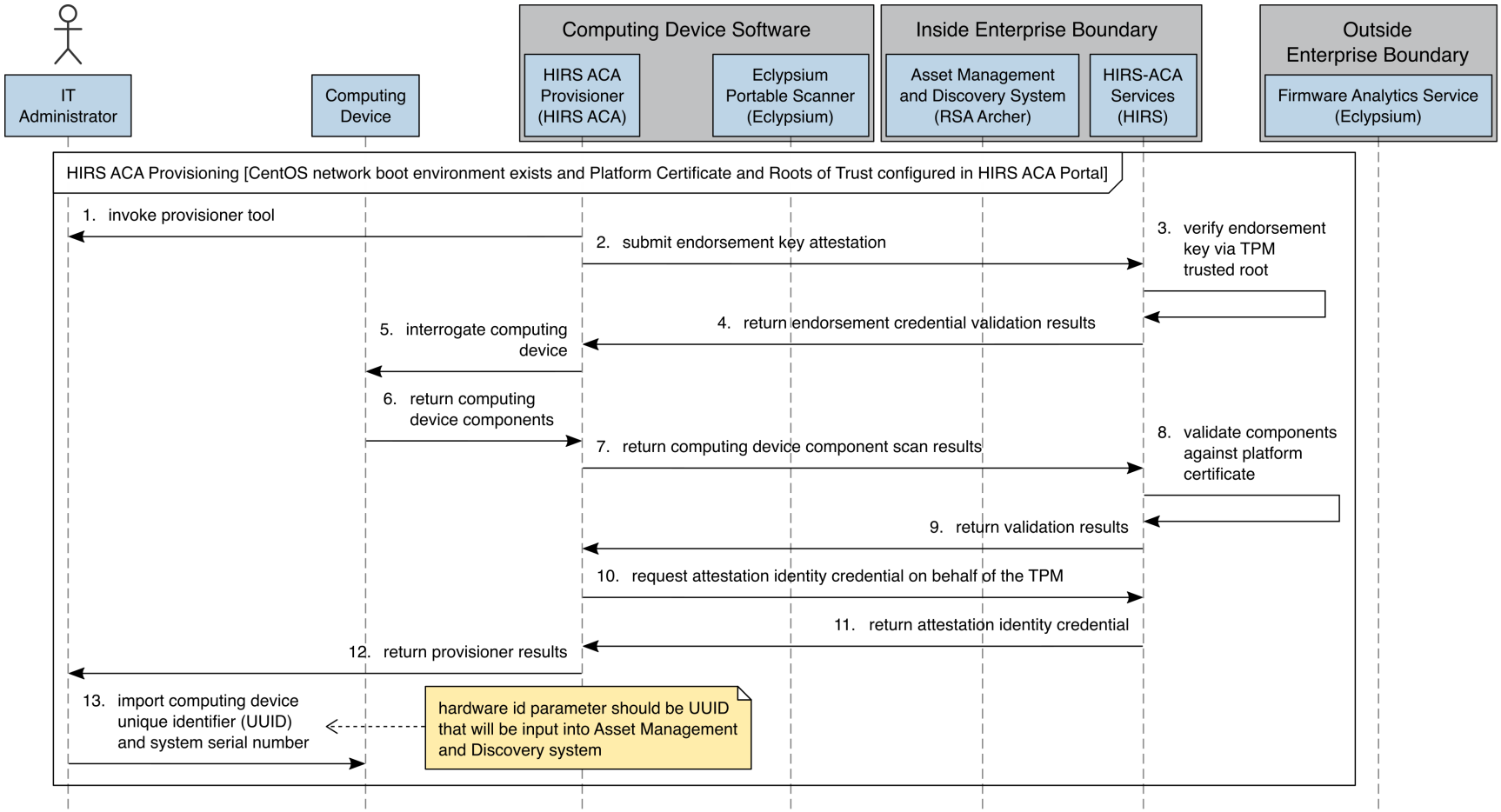


Figure 6-2 Dell Laptop Scenario 2 Part 2

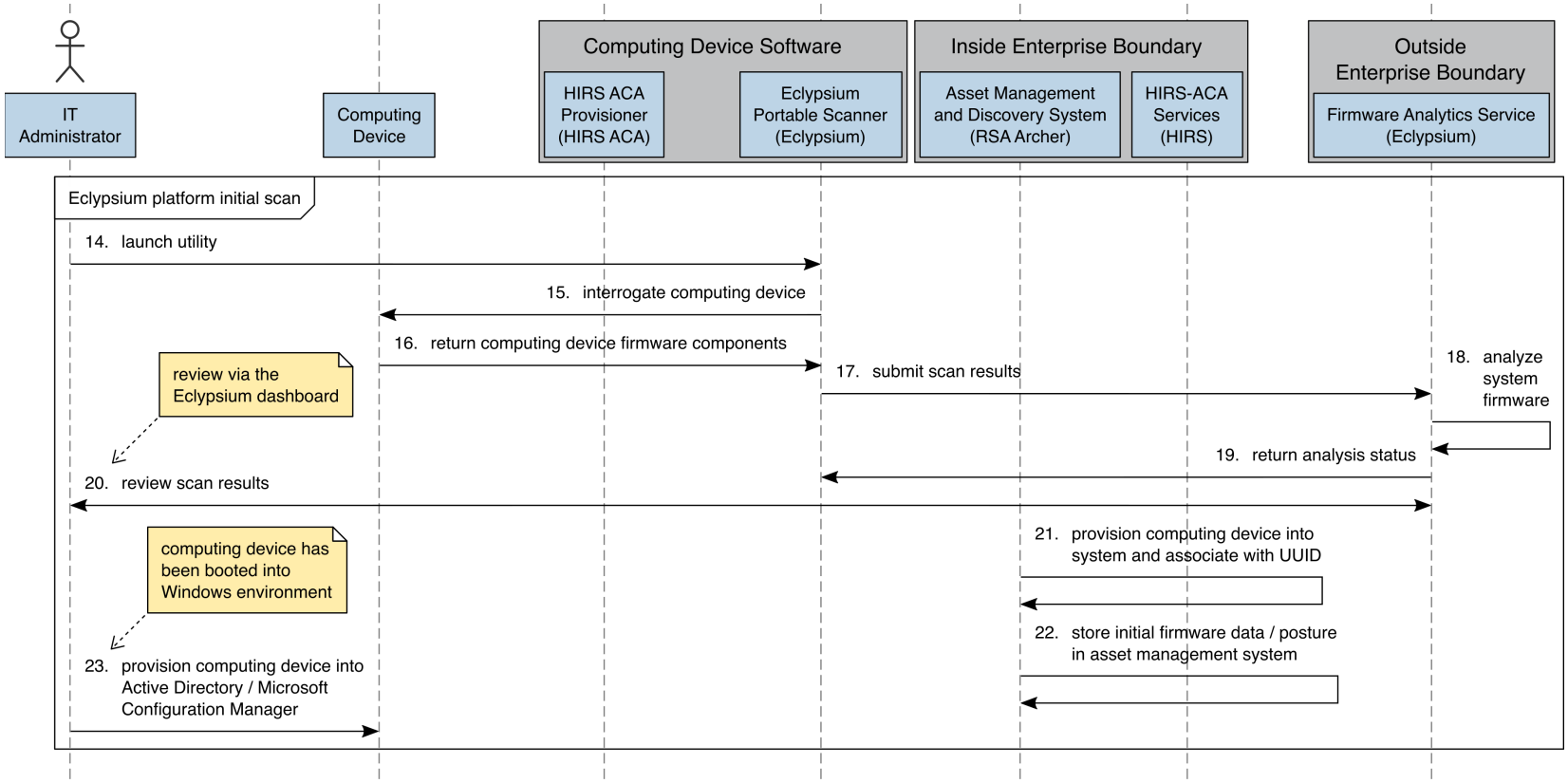


Figure 6-3 Intel Laptop Scenario 2 Part 1

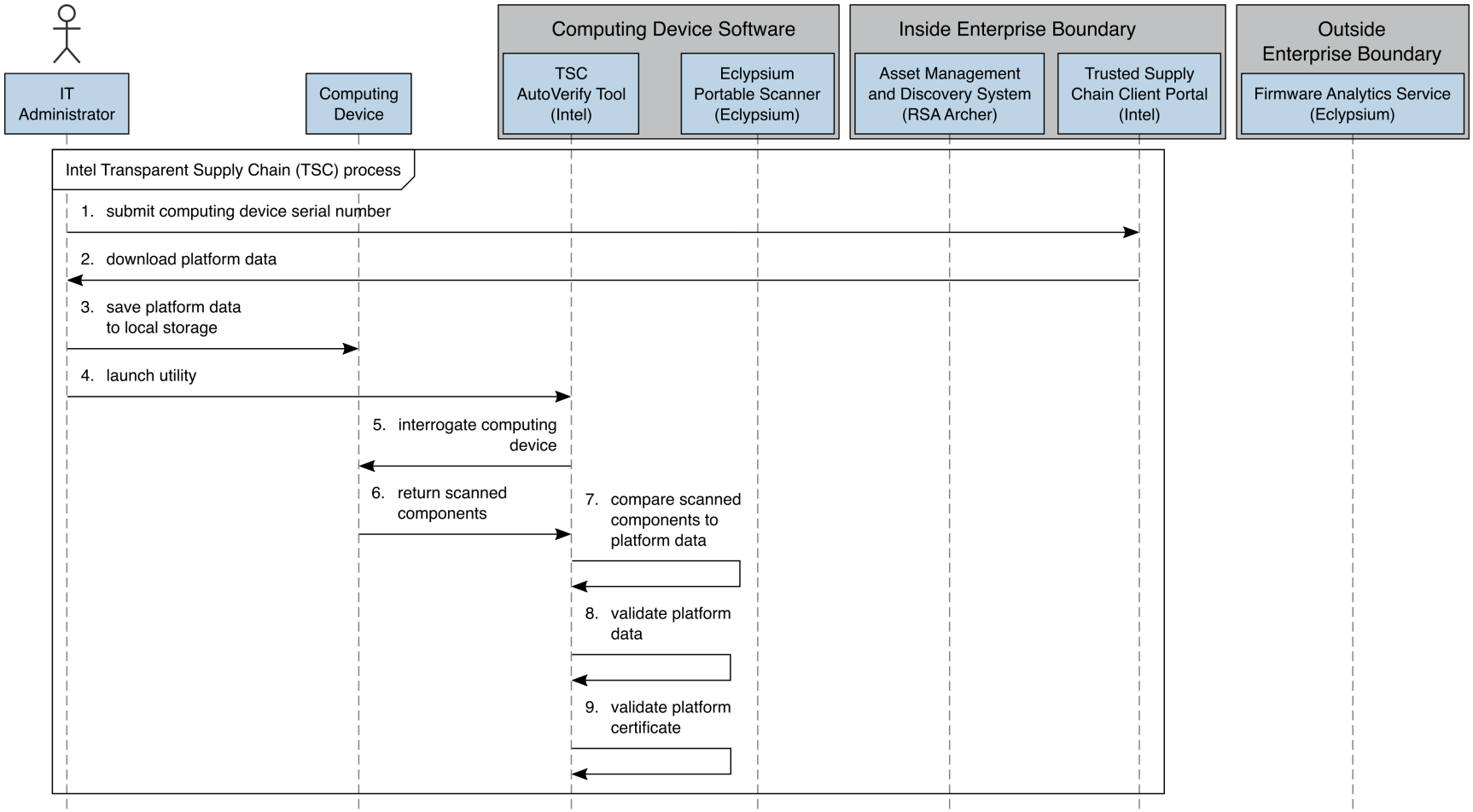


Figure 6-4 Intel Laptop Scenario 2 Part 2

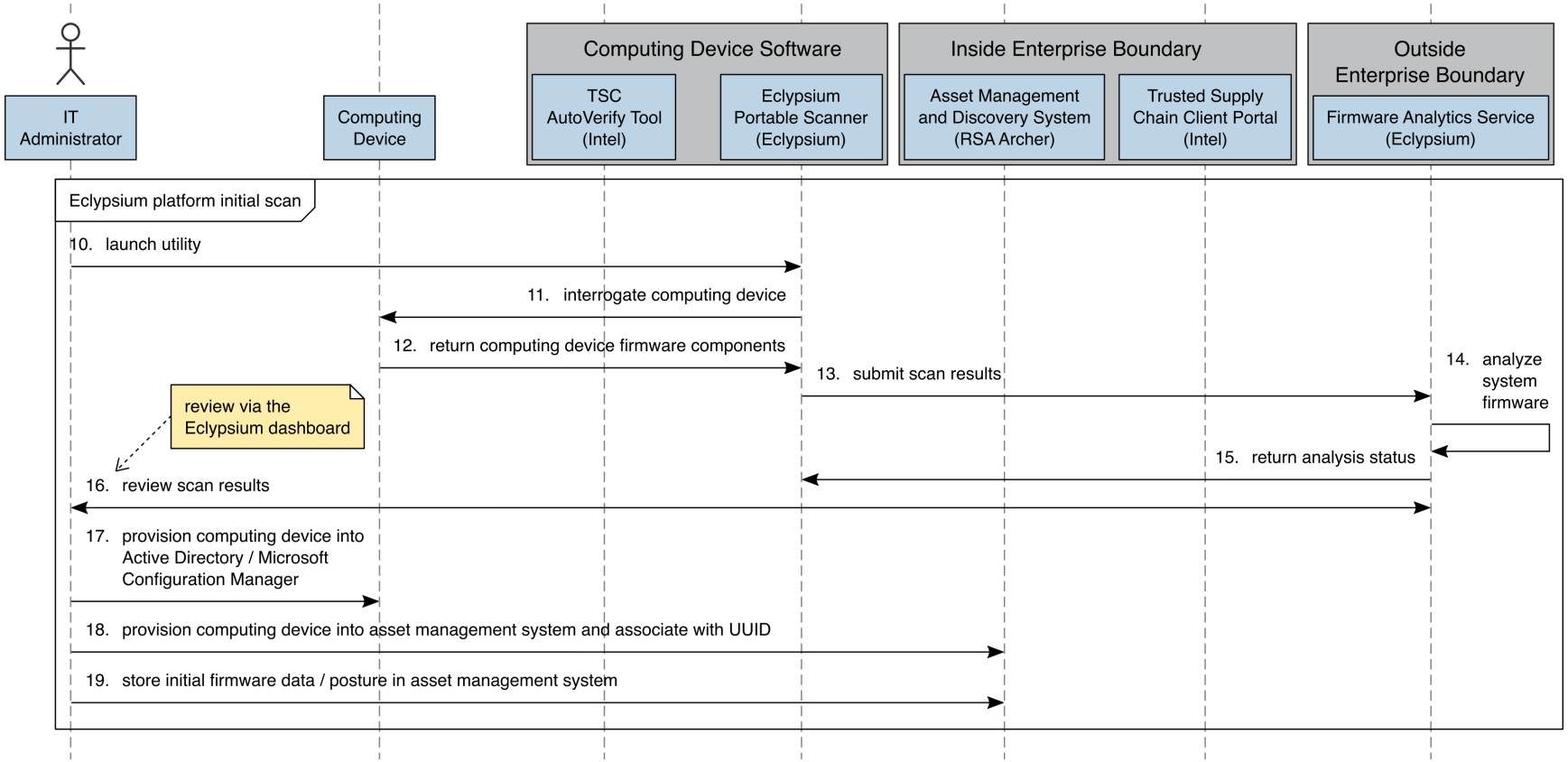


Figure 6-5 Intel Laptop Scenario 3