smart cities

MDPI

Article

CO-TSM: A Flexible Model for Secure Embedded Device Ownership and Management

Konstantinos Markantonakis [1,*,†], Ghada Arfaoui [2,†], Sarah Abu Ghazalah [3], Carlton Shepherd [4], Raja Naeem Akram [5] and Damien Sauveron [6]

[1] Information Security Group—Smart Card Centre, Royal Holloway, University of London, Egham TW20 0EX, UK
[2] Orange Laboratory, 35510 Cesson-Sévigné, France; ghada.arfaoui@orange.com
[3] Information Security and Cyber Security Unit, King Khaled University, Abha 62521, Saudi Arabia; sabugazalah@kku.edu.sa
[4] Department of Computer Science, University of Newcastle, Newcastle NE1 7RU, UK; carlton.shepherd@newcastle.ac.uk
[5] Department of Computer Science, University of Aberdeen, Aberdeen AB24 3FX, UK; raja.akram@abdn.ac.uk
[6] Department of Computer Science, XLIM, UMR CNRS 7252, University of Limoges, Avenue Albert Thomas, 87060 Limoges, France; damien.sauveron@unilim.fr
[*] Correspondence: k.markantonakis@rhul.ac.uk
[†] These authors contributed equally to this work.

Highlights:

What are the main findings?

- CO-TSM enables decentralised application management across smart cards, embedded devices, HCE-TEE smartphones, IoT devices, and RFID-enabled supply chains.
- The model enhances security through continuous evaluation and remote attestation while empowering users with greater device control.

What is the implication of the main finding?

- CO-TSM can revolutionize secure embedded device management by addressing market fragmentation and interoperability challenges.
- Its adoption could lead to more flexible, scalable, and user-centric approaches in managing secure applications across industries.

Abstract: The Consumer-Oriented Trusted Service Manager (CO-TSM) model has been recognised as a significant advancement in managing applications on Near Field Communication (NFC)-enabled mobile devices and multi-application smart cards. Traditional Trusted Service Manager (TSM) models, while useful, often result in market fragmentation and limit widespread adoption due to their centralised control mechanisms. The CO-TSM model addresses these issues by decentralising management and offering greater flexibility and scalability, making it more adaptable to the evolving needs of embedded systems, particularly in the context of the Internet of Things (IoT) and Radio Frequency Identification (RFID) technologies. This paper provides a comprehensive analysis of the CO-TSM model, highlighting its application in various technological domains such as smart cards, HCE-based NFC mobile phones, TEE-enabled smart home IoT devices, and RFID-based smart supply chains. By evaluating the CO-TSM model's architecture, implementation challenges, and practical deployment scenarios, this paper demonstrates how CO-TSM can overcome the limitations of traditional TSM approaches. The case studies presented offer practical insights into the model's adaptability and effectiveness in real-world scenarios. Through this examination, the paper aims to underscore the CO-TSM model's role in enhancing scalability, flexibility, and user autonomy in secure embedded device management, while also identifying areas for future research and development.

Keywords: CO-TSM; NFC; smart cards; IoT; RFID; security; application management

check for updates

Citation: Markantonakis, K.; Arfaoui, G.; Ghazalah, S.A.; Shepherd, C.; Akram, R.N.; Sauveron, D. CO-TSM: A Flexible Model for Secure Embedded Device Ownership and Management. *Smart Cities* **2024**, *7*, 2887–2909. https://doi.org/10.3390/smartcities7050112

Academic Editor: Pierluigi Siano

Received: 28 June 2024
Revised: 23 August 2024
Accepted: 12 September 2024
Published: 8 October 2024

1. Introduction

The rapid evolution of embedded device technologies, particularly in Near Field Communication (NFC), Internet of Things (IoT), and Radio Frequency Identification (RFID), has created a pressing need for more flexible and scalable management solutions. Traditional Trusted Service Manager (TSM) models, while effective in certain contexts, have been increasingly challenged by market fragmentation and the limited interoperability of multiapplication smart cards and NFC-enabled devices [1–6].

This paper revisits the Consumer-Oriented Trusted Service Manager (CO-TSM) model, originally introduced as a solution to these challenges. The CO-TSM model builds on the foundational principles of TSM by decentralising control and enhancing flexibility, allowing for broader adoption across diverse technological ecosystems. The CO-TSM model integrates the Issuer Centric Smart Card Ownership Model (ICOM) and the User Centric Smart Card Ownership Model (UCOM), addressing the needs of a wide range of stakeholders, from end-users to service providers.

The objective of this paper is to provide an in-depth examination of the CO-TSM model's applications, implementation challenges, and potential benefits across various domains, including HCE-based NFC mobile phones, TEE-enabled IoT devices, and RFID-based smart supply chains. By leveraging the strengths of CO-TSM, this paper aims to demonstrate how it can serve as a robust alternative to traditional TSM approaches, particularly in contexts where scalability, flexibility, and user autonomy are paramount.

This paper is structured as follows: Section 2 examines the traditional TSM architecture, outlining its foundational role in the development of the CO-TSM model. Section 3 offers a comparative analysis of various TSM-based deployment models, highlighting the limitations and establishing the need for a more flexible and user-centric approach. In Section 4 the paper delves into the CO-TSM model, its architecture, key features, and deployment considerations, followed by detailed case studies and an analysis of its deployment across different technological ecosystems in Section 5. The paper then discusses the limitations of the CO-TSM model and identifies areas for future research in Section 6, concluding with a summary of the key findings and contributions in Section 7.

Through this exploration, the paper aims to contribute to the ongoing discourse on secure embedded device management by demonstrating the practical implications and benefits of the CO-TSM model in addressing the limitations of traditional TSM approaches.

2. Trusted Service Manager (TSM)

The Trusted Service Manager (TSM) has historically been integral in the management of secure applications on smart cards and NFC-enabled devices. As an intermediary, the TSM facilitates interactions between service providers and the secure elements within devices, managing application lifecycles, ensuring secure communication, and maintaining compliance with security policies [7–11].

2.1. Overview of TSM Architecture

The architecture of TSMs is structured around centralised control, where a single entity manages the secure deployment and operation of applications across multiple service providers and devices. This centralisation allows for streamlined application management but also introduces significant challenges, particularly in terms of scalability, interoperability, and market fragmentation.

The typical TSM deployment, as illustrated in Figure 1, shows the TSM acting as a trusted intermediary among various stakeholders such as Mobile Network Operators (MNOs), banks, and service providers. Each of these stakeholders requires secure access to the applications hosted on smart cards or NFC-enabled devices. While this model ensures high security and control, it often leads to market fragmentation, as each TSM may operate in isolation from others, limiting cross-platform interoperability and user flexibility.

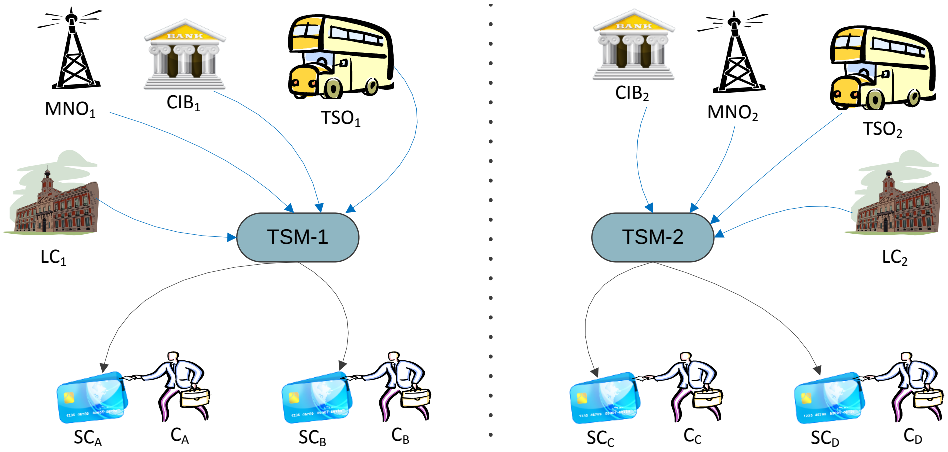


Figure 1. Generic TSM deployment architecture.

The limitations of traditional TSM architectures, particularly regarding scalability and flexibility, have led to the development of the Consumer-Oriented Trusted Service Manager (CO-TSM) model. The CO-TSM model was introduced to address these challenges by decentralising control and allowing users and service providers more autonomy in managing applications on secure elements.

Unlike the centralised TSM, the CO-TSM framework allows for a more distributed approach, where multiple TSMs can interact in a federated manner, giving users greater flexibility in choosing service providers and managing applications across different platforms. This model builds on the strengths of traditional TSMs while mitigating their limitations by fostering a more open and scalable ecosystem.

While the CO-TSM model represents a significant advancement, the principles of traditional TSMs remain relevant. The secure management of applications and the trust frameworks established by TSMs are foundational to the CO-TSM model. However, CO-TSM extends these principles by enabling greater interoperability and user control, which are critical in the context of modern, interconnected devices such as those found in IoT and smart home environments.

2.2. Summary of Key Points

In summary, the traditional TSM model has provided a robust framework for secure application management, but its limitations necessitated the evolution towards a more flexible and scalable approach. The CO-TSM model, which builds upon the established TSM principles, offers enhanced capabilities suited to contemporary technological ecosystems, where decentralisation, interoperability, and user autonomy are increasingly important.

3. Analysis of TSM-Based Deployment Models

The Trusted Service Manager (TSM) model has played a crucial role in managing the lifecycle of applications on NFC-enabled devices and multi-application smart cards. However, traditional TSM models, such as the Issuer Centric Smart Card Ownership Model (ICOM) and the User Centric Smart Card Ownership Model (UCOM), face limitations that necessitate more flexible and scalable alternatives.

3.1. Traditional and Evolving TSM Models

Traditional TSM models, including ICOM and UCOM, represent the two primary approaches to smart card application management. In the ICOM, the card issuer maintains control over the smart card and its applications, offering strong security guarantees but limiting flexibility. Conversely, the UCOM gives more control to the end-user, enhancing flexibility but complicating the enforcement of consistent security standards.

To address these limitations, organisations like GlobalPlatform and GSMA have proposed variations of the TSM model. GlobalPlatform's proposals, including simple, delegated, and authorised modes, aim to balance centralised control with the flexibility required by service providers. The authorised mode, in particular, allows independent TSMs to manage specific applications without the need for constant approval from the card issuer or Mobile Network Operator (MNO). These models are illustrated in Figure 2, which shows the varying degrees of control and flexibility offered by each mode.

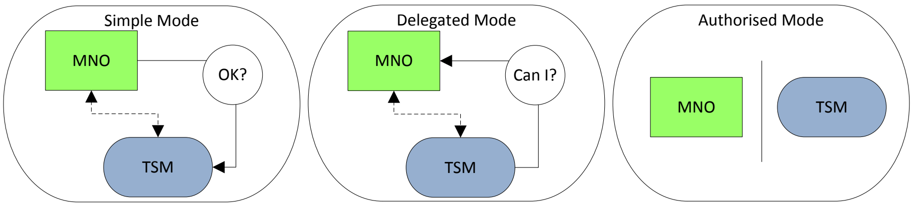


Figure 2. The TSM Deployment Models proposed by GlobalPlatform.

Similarly, the GSMA's TSM models emphasise the role of MNOs in managing NFC services, ranging from fully MNO-controlled TSMs to more aggregated models where third-party TSMs act as intermediaries between service providers and MNOs. These models are depicted in Figures 3–5, each representing a different level of MNO involvement and control over the TSM operations.

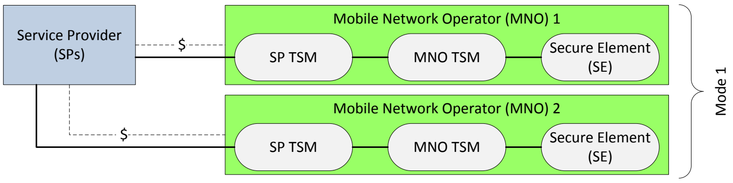


Figure 3. GSMA's TSM Proposal: Mode 1.

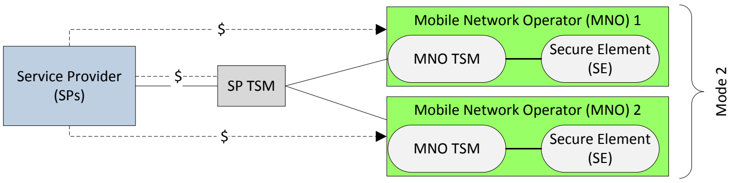


Figure 4. GSMA's TSM Proposal: Mode 2.

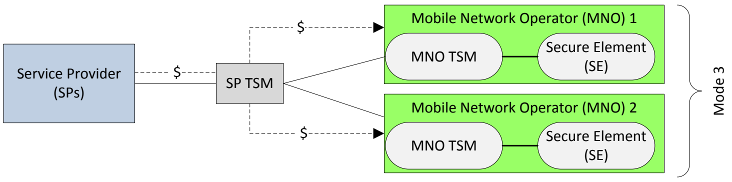


Figure 5. GSMA's TSM Proposal: Mode 3.

3.2. Challenges and Limitations of TSM Models

Despite the advancements introduced by GlobalPlatform and GSMA models, several challenges remain unresolved. Market fragmentation is a significant issue, as centralised control by issuers or MNOs can lead to fragmented markets, limiting consumer choice and requiring service providers to establish multiple partnerships to reach a broad audience.

Scalability is another challenge, as the centralised nature of traditional TSM models can create bottlenecks, particularly as the number of connected devices and services grows. This can hinder the deployment of new services and complicate the management of large-scale networks.

Limited flexibility is also a concern. Traditional TSM models often lack the flexibility needed to accommodate the diverse needs of modern consumers and service providers, potentially slowing the deployment of innovative services. Furthermore, these models tend to focus on the needs of issuers and service providers, often neglecting the consumer's role in managing and controlling their devices and applications.

3.3. Summary of Key Points

This analysis of TSM-based deployment models highlights several critical points that underline the ongoing challenges in managing applications on NFC-enabled devices and multi-application smart cards:

- Market Fragmentation:Traditional TSM models, with their centralised control structures, contribute to market fragmentation. This fragmentation limits consumer choice and forces service providers to engage in multiple partnerships to reach a broad audience, thereby restricting the overall interoperability and adoption of smart card technologies.
- Scalability Issues: As the number of connected devices and services continues to grow, the centralised nature of traditional TSM models poses significant scalability challenges. These bottlenecks hinder the deployment of new services and complicate the management of large-scale networks, making it difficult to meet the demands of modern, interconnected environments.
- Lack of Flexibility: Traditional TSM models often fail to accommodate the diverse needs of modern consumers and service providers. Their rigid structures can slow the deployment of innovative services and typically prioritise the needs of issuers and service providers over those of end-users, limiting consumer empowerment and control over their devices.
- Need for User-Centric Approaches: The limitations of traditional TSM models underscore the need for a more flexible and user-centric approach to smart card application management. Such an approach should empower consumers, enhance interoperability, and support the seamless integration of diverse services and devices.

These key points emphasise the necessity of evolving beyond traditional TSM models toward more adaptable solutions like the Consumer-Oriented Trusted Service Manager (CO-TSM) model. The next section will delve into the CO-TSM model, focusing on its architecture, implementation, and practical applications in various technological contexts.

4. Consumer-Oriented Trusted Service Manager Model

This section discusses the Consumer-Oriented Trusted Service Manager (CO-TSM) model, its architecture, key features, and deployment considerations.

4.1. Architecture

The CO-TSM model builds upon the existing Trusted Service Manager (TSM) framework with a key enhancement as shown in Figure 6: it allows for application installation from non-partner organisations, provided they meet the security and business requirements of the smart card. This model ensures that smart card security requirements are met and verified, regardless of whether the application provider is a partner of the CO-TSM.

Key factors driving innovation in this space include:

(a) The threat of new entrants
(b) The threat of substitute products or services
(c) Consumer power (culture)

The advent of NFC-enabled smartphones presents an opportunity to unify multiple services on a single smart card. The CO-TSM model addresses concerns about the role and executing entity of the TSM by being scalable, flexible, and focused on consumer needs.

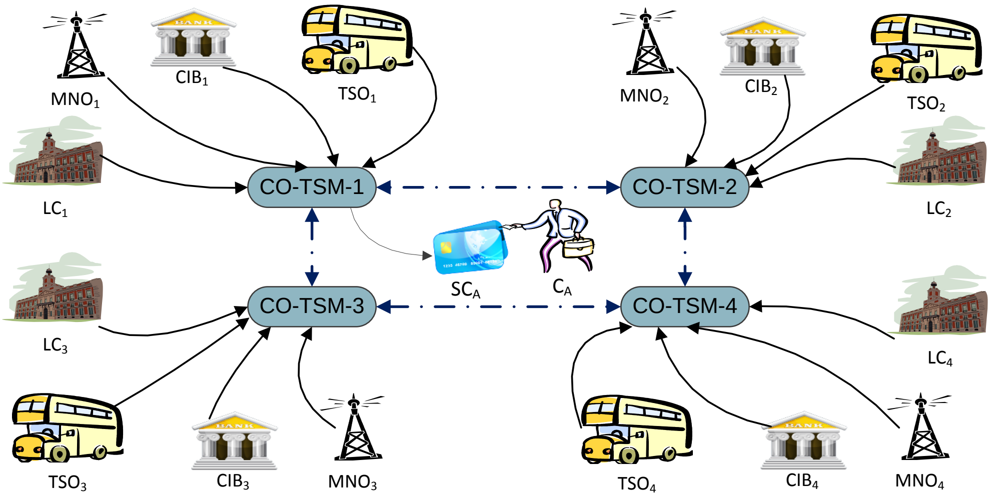


Figure 6. Overview of the Consumer-Oriented Trusted Service Manager (CO-TSM) model.

Key features of the CO-TSM model include:

[F1] Management of relationships between card issuers, service providers (SPs), and users, acting as a neutral broker to protect each stakeholder's interests.
[F2] Serving as a security attestation and validation broker, ensuring that smart cards meet SP security requirements.
[F3] Ensuring that applications do not compromise smart card integrity.
[F4] Users' freedom to install any application, regardless of the SP's membership in any CO-TSM.
[F5] Users' ability to acquire their own smart card and delegate its management to a CO-TSM.
[F6] Users' privilege to choose and switch CO-TSMs, providing flexibility and control over their smart card management.

4.2. Deployment Challenges and Opportunities

The CO-TSM model allows user choice to install applications from any SP, provided the smart card's security is validated. Several challenges arise with this model:

1. Ensuring smart card security and providing assurances to SPs without direct agreements.
2. Establishing secure and trusted protocols for application downloads, including remote security attestation, validation, and fee processing.
3. Enabling users to manage applications and fulfil their requests for installations and deletions.

The CO-TSM model extends traditional Issuer Centric Ownership Model (ICOM) approaches by incorporating user rights and eliminating the need for offline partnerships between CO-TSMs and SPs. By supporting all key features mentioned earlier, it aligns closely with the User Centric Ownership Model (UCOM), providing a collaborative and ubiquitous solution.

4.3. Comparing ICOM- and UCOM-Based CO-TSM

Integrating CO-TSM into the ICOM model requires including consumers as significant stakeholders. The GlobalPlatform Consumer-Centric Model (GP-CCM) outlines principles for consumer involvement in ICOM. However, it does not fully support a collaborative and ubiquitous CO-TSM. Table 1 provides a comparison between ICOM- and UCOM-based CO-TSM approaches:

Table 1. Comparison of ICOM- and UCOM-based CO-TSM.

Aspect	ICOM-Based CO-TSM	UCOM-Based CO-TSM
Security Assurance for SPs	Relies on evaluation and certification at issuance and installation	Includes mechanisms for constant security evaluation and potential revocation
Detecting Simulator Attacks	Not fully addressed	Proposes countermeasures using remote attestation
Addressing Parasite Application Issues	Needs further development	Proposes countermeasures
Flexible Charging for Application Installations	Limited by offline relationships	Supports online fee processing during installation
Secure Application Sharing	Uses traditional firewalls	Proposes modifications to the traditional firewall mechanism
Platform Protection	Limited	Proposes run-time security mechanisms to prevent malicious behaviour
Recovery Mechanism for Lost Smart Cards	Not specifically addressed	Proposes an instant recovery mechanism

By supporting all requirements mentioned earlier, the CO-TSM provides a collaborative and ubiquitous solution, benefiting from the robust architecture of UCOM while addressing the limitations of traditional TSM models.

4.4. Summary of Strengths and Weaknesses

The Consumer-Oriented Trusted Service Manager (CO-TSM) model offers a compelling alternative to traditional smart card management approaches, particularly in its ability to enhance flexibility, security, and user control—as listed in the Table 2. However, its implementation also presents certain challenges that need to be carefully considered. The following table outlines the key strengths and weaknesses of the CO-TSM model.

Table 2. Summary of Strengths and Weaknesses of the CO-TSM Model.

Category	Strengths	Weaknesses
Flexibility	Users can install applications from any Service Provider (SP), regardless of partnership with the CO-TSM.	The increased flexibility might introduce new attack vectors that need to be carefully addressed.
Security	Incorporates constant security evaluation and remote attestation mechanisms.	Requires significant changes to existing smart card architectures and protocols.
User Empowerment	Allows users to choose and switch CO-TSMs, providing greater control over their smart card management.	The increased control given to users necessitates better education about security implications.
Scalability	Supports online fee processing and eliminates the need for offline partnerships between CO-TSMs and SPs.	Implementing a unified CO-TSM model across different stakeholders may require extensive standardisation efforts.
Comprehensive Approach	Addresses issues such as parasite applications and platform protection that are not fully resolved in traditional models.	May face resistance from established players in the smart card ecosystem who benefit from current ICOM-based models.

The CO-TSM model represents a forward-thinking approach that aligns with the growing demand for more adaptable and user-centric smart card management systems. However, successfully deploying this model will require overcoming several technical, educational, and standardisation challenges.

5. Case Studies of CO-TSM Deployments

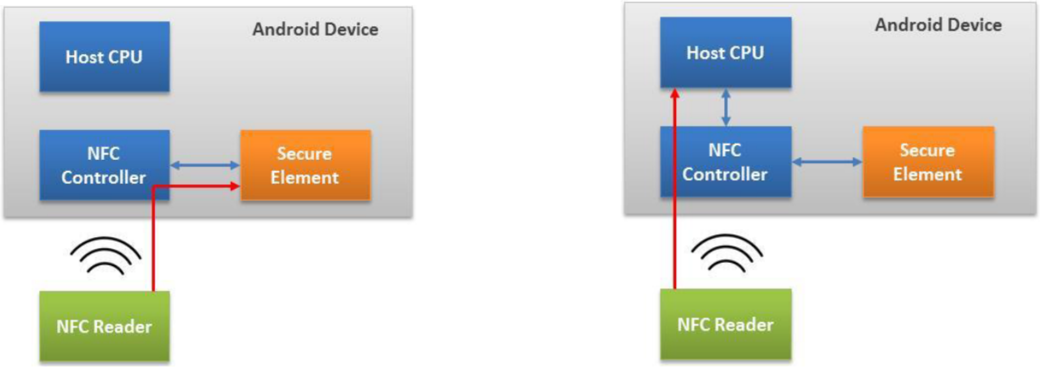
The proposed CO-TSM model can easily be extended as a flexible and scalable solution for HCE-TEE smartphones, IoT, and smart supply-chain deployments.

5.1. CO-TSM UCOM Based HCE-TEE Smart Phone Deployment

This section explores the use of an open CO-TSM model for issuing and deploying applications in Host Card Emulation (HCE) environments protected by a Trusted Execution Environment (TEE).

Host Card Emulation (HCE) [12,13] enables mobile devices to emulate smart cards independently of Secure Elements (SEs) using libraries and APIs implemented in the host operating system. HCE allows any mobile application to exchange APDUs with an NFC reader and has been supported by major payment networks since 2014.

In HCE, the NFC controller uses a routing table with Application IDentifiers (AIDs) to direct incoming messages to either the active SE or host OS, as shown in Figure 7. While HCE offers reduced development costs and shorter market lead times compared to SEs, it faces challenges in user experience, security, and availability. To address these issues, a HCE-TEE solution using a local TEE to store credentials and perform security-critical operations is proposed.



(**a**) SE-based Emulation (**b**) HCE-based Emulation

Figure 7. NFC-enabled Device Using SE- and HCE-based Card Emulation(Source: Smart Card Alliance [13]).

A Trusted Execution Environment (TEE), as standardised by GlobalPlatform [14–16] is a hardware-assisted secure environment that executes alongside a standard mobile operating system. The TEE operates using trusted components partitioned from the native OS through hardware-enforced access control, as shown in Figure 8.

The GlobalPlatform TEE software architecture (Figure 9) illustrates how the TEE OS manages hardware resources and facilitates communication between the Rich Execution Environment (REE) and Trusted Applications (TAs).

TEEs offer secure boot, isolation, and secure storage capabilities. However, they are typically certified to a lower evaluation assurance level (EAL2) compared to smart cards and SEs (EAL4). TEEs are primarily designed to defend against privileged REE software attacks rather than complex hardware attacks.

5.1.1. CO-TSM UCOM-Based HCE-TEE Architecture

The HCE-TEE ecosystem can be modelled similarly to a smart card ecosystem, as shown in Figure 10. This model includes roles such as end-user, chip manufacturer, device manufacturer, client applications manager, trusted applications manager, and TEE manager.

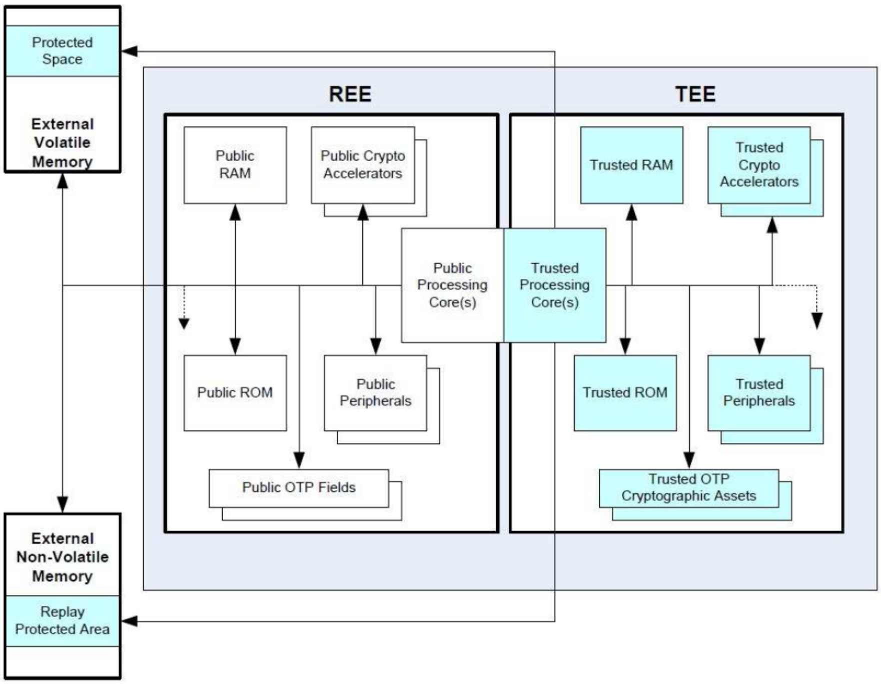

Protected Space
External Volatile Memory
REE
TEE
Public RAM
Public Crypto Accelerators
Trusted RAM
Trusted Crypto Accelerators
Public Processing Core(s)
Trusted Processing Core(s)
Public ROM
Public Peripherals
Trusted ROM
Trusted Peripherals
Public OTP Fields
Trusted OTP Cryptographic Assets
External Non-Volatile Memory
Replay Protected Area

Figure 8. GlobalPlatform TEE hardware architecture (Source: GlobalPlatform Specification [15]. Trusted components shown in blue; untrusted units are uncoloured.

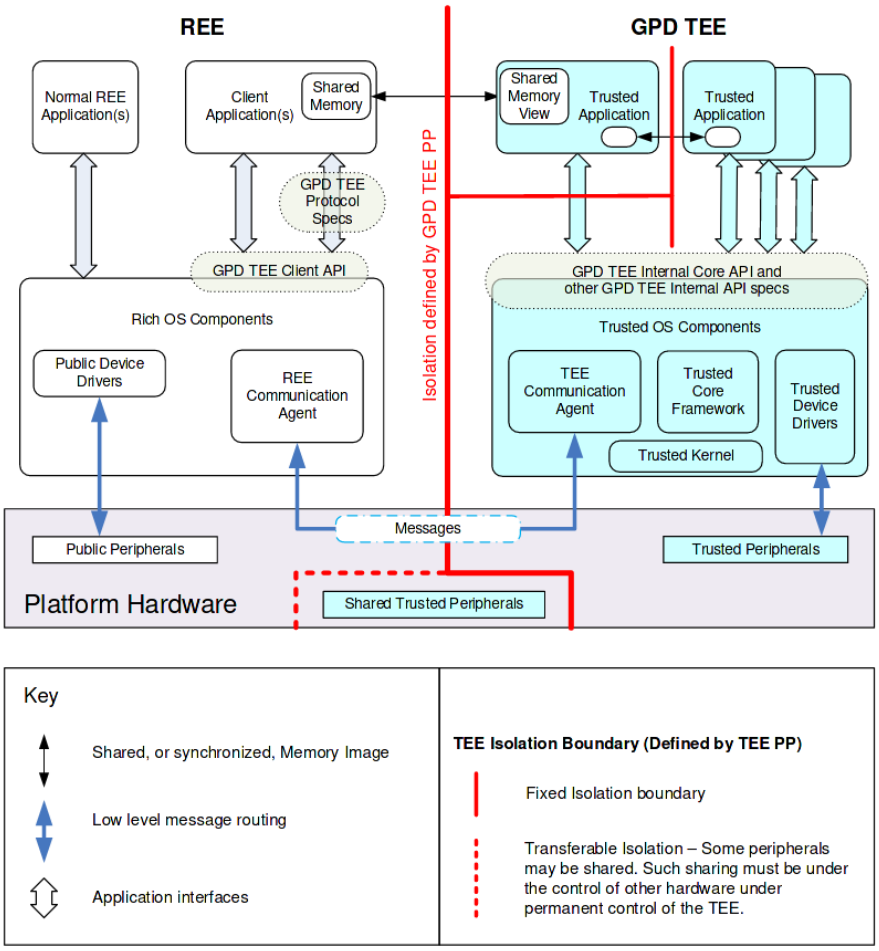


Figure 9. GlobalPlatform TEE software architecture (Source: GlobalPlatform Specifiation [16].

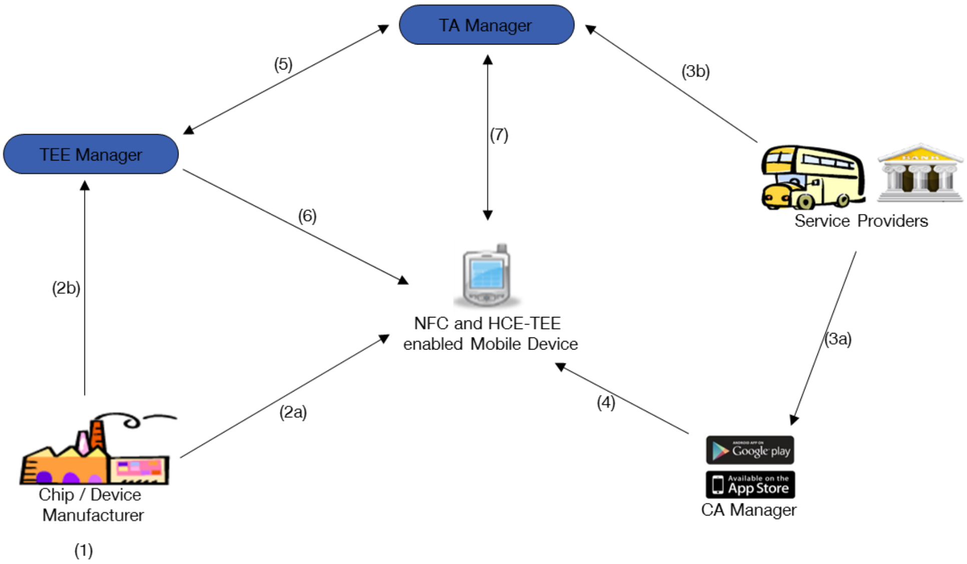


Figure 10. Ecosystem of a HCE-TEE enabled Device.

The CO-TSM UCOM model can be applied to HCE-TEE-enabled devices, potentially with fewer historical barriers than in traditional smart card ecosystems. Key distribution and management in this model involve several steps:

1. Establishing a unique per-chip root key for each TEE.
2. Device delivery and preliminary key distribution.
3. Application development and distribution.
4. TEE initialisation and key establishment.
5. CO-TSM authorisation and key management.
6. Update TEE Manager and HCE-TEE key management.
7. Update TA Manager and HCE-TEE key management.

This approach provides a framework for secure application deployment in HCE-TEE environments using the CO-TSM UCOM model, leveraging the security benefits of TEEs while addressing the flexibility needs of modern mobile ecosystems.

5.2. CO-TSM UCOM-Based Smart Home

We now describe a second case study for secure embedded device management under the CO-TSM UCOM model in smart home environments.

5.2.1. Smart Home Architecture

A smart home comprises Internet- and locally-connected devices that monitor and control its ambient environment, such as lighting; energy consumption; audio and video devices; smart assistants; security equipment, e.g., cameras and access control and climate controls. Users may monitor and actuate devices directly from a master control device, such as the homeowner's mobile phone, smartwatch or tablet (Figure 11). Alternatively, devices may autonomously react to environmental conditions; for example, a smart thermostat reducing the temperature if it exceeds the user's desired level of comfort. Smart homes empower users to optimise comfort and costs, such as electricity expenditure, as well as offering tools for surveillance and physical security within the home.

Smart home devices access the Internet using a gateway, e.g., home router. Devices may connect directly to this gateway or, in certain instances, through an intermediate hub that controls multiple descendent devices. Lighting networks are a common example of the latter case, where the attributes of multiple individual light bulbs—colour, brightness, and on/off status—can be orchestrated from a control hub. The device architecture typically centres around an embedded system-on-chip (SoC). The SoC may host a microcontroller for limited tasks, e.g., collecting sensor measurements and activating electrical relays, or an application processor for hosting a fully-fledged operating system. ARM-based SoCs, used by 90% of mobile and IoT devices, support TEEs for all but the most limited microcontroller CPUs using ARM TrustZone [17,18]. TrustZone is the predominant technology for instantiating the GlobalPlatform TEE on mobile and embedded devices [19]. TEEs have been used for various applications in smart home environments, including audio/video digital rights management (DRM), e.g., WideVine, and storing and authenticating user biometric credentials securely [18,20,21].

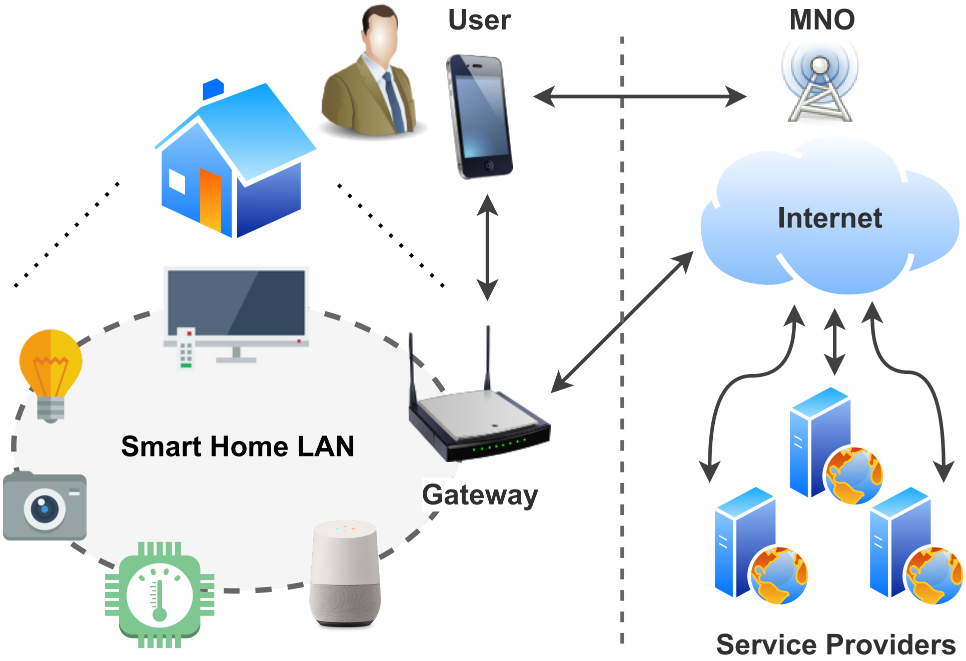


Figure 11. Generic smart home architecture.

Device services are developed by heterogeneous and often competing manufacturers. Users access control/monitor functionality by installing an SP's respective application(s) to their phone and/or gateway. Depending on the service, this can enable users to control cameras, heating and air conditioning units within or outside the smart home's LAN. The management of device services is shared between SPs and users. SPs serve over-the-air (OTA) software and firmware updates, and administer TEE-based services using a typical TSM architecture as per the GlobalPlatform TEE TMF specifications. Users are involved by enrolling and removing new devices to and from the network using, for instance, a gateway mobile application installed on their smartphone.

The security and privacy of smart home devices have attracted significant attention from academia and industry [22–24]. This follows many high-profile security flaws discovered in sensitive devices and services, e.g., baby monitors, have attracted attracting international publicity [25–27]. In particular, economic incentives to deliver devices rapidly to market at low per-unit costs has prompted concerns about the rigour of their security measures [28,29].

In theory, TEEs are an attractive low-cost option for strong hardware-assisted security. This stems from their mass-market availability, low physical footprint, and near-native performance. In reality, we argue that the traditional TSM model, as described in the GlobalPlatform TEE TMF, is a major barrier to flexible and consumer-centric TEE-enabled smart home devices. A variety of TSMs may exist in a smart home environment with different device manufacturers, chip manufacturers, service providers, and TEE developers. In this situation, users are limited to the applications and services available from a TSM, thus cementing existing concerns regarding IoT interoperability, flexibility, and monopolisation [30].

5.2.2. CO-TSM UCOM-Based Smart Home Architecture

Our CO-TSM model can mitigate these drawbacks by allowing the installation and management of user-desired applications on smart home TEEs. This overcomes the limitations of the traditional TSM model that exacerbate market fragmentation (Section 2).

A CO-TSM smart home architecture involves the same entities as the HCE-TEE model (Section 5.1.1), with the exception that multiple end-user devices and device and chip manufacturers are present. This places a greater key management burden on the TEE Manager to manage a substantially large number of devices with disparate chips. Otherwise, the process is largely the same. Devices are set up in the same way as the HCE-TEE model; that is, each TEE is assumed to have a unique per-chip key, which is delivered in a disabled mode to the end-user. Service providers then develop client and trusted applications for each smart home device, which are uploaded to the client and trusted application managers, e.g., smart home application stores. The end-user downloads the client from the client applications manager through a control device, e.g., smartphone or tablet, and triggers the TA and TEE initialisation. Here, the TEE Manager then initialises the TEE root key and a cryptographic key for the CO-TSM to communicate with the TEE. In the same way, the CO-TSM downloads applications to its region on the TEE and establishes keys for managing these TAs.

Using this model, the CO-TSM is still able to fulfil the key services demanded by smart home devices, such as firmware and software OTA updates to vulnerable devices. The CO-TSM model provides additional flexibility in allowing new devices to be added to the smart home if the above procedure is followed. If the user wishes to change or remove the TSM—for example, if the device is sold on the resale market—then the same ownership management procedure can be used from Section 4.1 to transfer ownership and management between Users.

5.3. CO-TSM UCOM-Based RFID Architecture for Smart Supply Environments

This section delves into the CO-TSM UCOM-based RFID architecture, focusing on its application within modern smart supply settings. Integrating RFID technology in these environments unlocks transformative potential for enhanced efficiency, accuracy, and real-time tracking of goods. However, this approach also presents unique challenges and limitations to overcome.

5.3.1. What Are Smart Supply Environments?

Smart supply environments represent a revolutionary shift in supply chain management, leveraging cutting-edge technologies like RFID to optimise efficiency, accuracy, and the real-time tracking of goods throughout the entire supply chain—as illustrated in the Figure 12. This approach involves seamlessly integrating digital systems into every aspect of operations, from manufacturing and warehousing to logistics and retail [31]. The core objective is to establish a fully connected, transparent, and highly efficient supply network.

Example: Imagine a scenario where a shipment of temperature-sensitive pharmaceuticals is equipped with RFID tags. These tags not only track the location of the shipment but also monitor the surrounding temperature in real-time. These data can be used to alert logistics providers of any potential deviations from optimal storage conditions, enabling them to take immediate corrective action and prevent spoilage.

5.3.2. RFID Technology and Smart Supply Architecture

Radio Frequency Identification (RFID) is a wireless technology that utilises electromagnetic fields to communicate unique identifiers stored within microchips attached to objects, animals, or individuals. RFID systems consist of three primary components: RFID tags, RFID readers, and middleware. RFID tags contain a microchip and antenna, classified as passive (powered by a reader's signal) or active (containing a battery). RFID readers generate radio waves to power and interrogate tags within their range, capturing the embedded identification data. The role of middleware involves translating raw RFID data into a usable format for business applications. Compared to traditional barcode technology, RFID offers superior advantages such as non-line-of-sight operation, simultaneous tag reading, and extended data capacity.

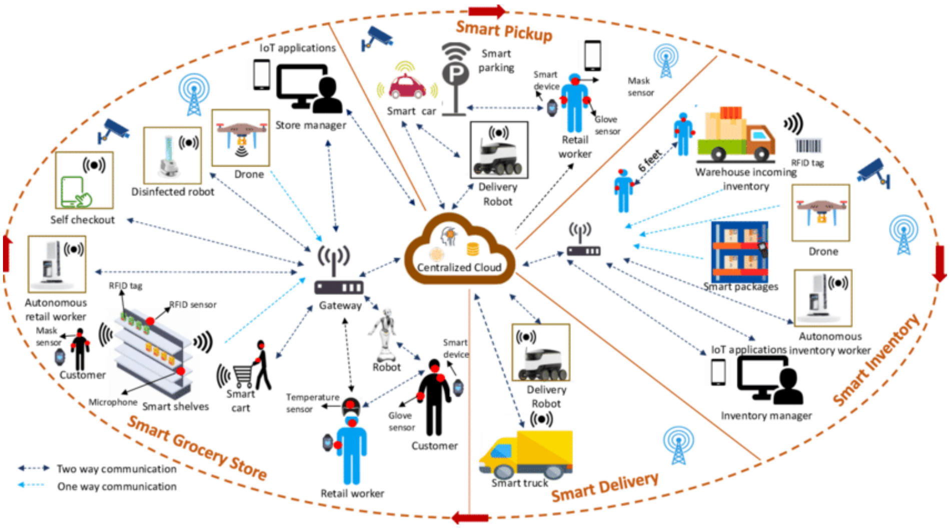


Figure 12. Illustrative example of a smart supply chain with integrated RFID technology (Source: Gupta et al. [32].

RFID integration fosters efficiency, visibility, and accuracy throughout various stages of the supply chain. In inventory management and tracking, RFID-tagged products and pallets allow for real-time monitoring of stock levels within warehouses and distribution centers [33]. This visibility results in proactive replenishment strategies and the reduction of out-of-stock situations. Similarly, RFID enables the tracking of high-value assets like equipment or reusable transport containers across their movements within the supply chain [34]. The data collected optimise the use of these assets and facilitates proactive loss prevention efforts.

During shipment, RFID offers capabilities for in-transit visibility of pallets or containers, along with the monitoring of critical environmental factors like temperature and humidity. This monitoring promotes adherence to optimal transport conditions, helping to detect potential product damage or tampering events. Lastly, RFID plays a role in anti-counterfeiting measures. Products incorporating unique RFID identifiers create barriers for counterfeiters to replicate, safeguarding supply chain integrity and promoting brand trust [31].

In supply chains, when ownership of products changes hands, updating RFID ownership information presents technical and security-related challenges. Central to efficient ownership transfer is maintaining data synchronisation and rigorous data management practices for seamless updates as assets change owners. Blockchain technology presents potential solutions, facilitating the reliable tracking of ownership changes through the use of decentralised ledgers [35]. RFID systems must also safeguard data privacy and security. Unauthorised access to sensitive ownership-related data or attempts to alter RFID records constitute supply chain integrity risks, making strong encryption and authentication protocols a necessity [33]. Scalability becomes an increasingly critical factor as RFID is incorporated into complex supply chains involving numerous stakeholders, thus highlighting the need for advanced management platforms.

The integration of RFID technology within a smart supply chain framework introduces unprecedented levels of automation, traceability, and real-time asset management. A notable and highly desirable property is the potential for frictionless ownership transfer of tagged assets along the supply chain. As devices seamlessly change hands from suppliers to manufacturers to distributors, a robust RFID ownership transfer mechanism promotes multiple advantages:

- Enhanced Asset Utilisation: Efficient ownership updates reflect the updated status of items in the supply chain, preventing assets from becoming ’lost’ or misallocated between entities. This promotes proactive optimisation with redeployments and rentals.
- Circular Economy Facilitation: RFID-enabled ownership information helps in the recovery, repurposing, and proper end-of-life disposal of assets. This supports a sustainable and waste-reductive circular economy model.
- Reduction of Carbon Footprint: Optimal asset utilisation and circular economy practices, powered by the data visibility fostered by RFID, directly contribute to reducing waste and greenhouse gas emissions associated with redundant manufacturing and resource depletion.
- Improved Collaboration and Trust: Transparent tracking of ownership promotes supply chain transparency, encouraging greater collaboration and building trust among stakeholders.

However, limitations arise when addressing ownership transfer in traditional RFID system architectures. Centralised ownership databases face inherent issues of scalability, susceptibility to security breaches, and the potential for single points of failure. These limitations are exacerbated in complex, multi-stakeholder supply chains.

This paves the way for considering the potential of decentralised technologies in facilitating RFID ownership transfer while mitigating the shortcomings of centralised systems. Could blockchain technology provide a framework for the development of a distributed, secure, and immutable record of ownership information, enabling smooth transitions across stakeholder boundaries without introducing potential bottlenecks?

5.3.3. Blockchain Technology

Blockchain technology offers a potentially transformative solution to the limitations inherent in centralised ownership management within RFID-enabled supply chains. At its core, a blockchain serves as a decentralised, tamper-resistant digital ledger distributed across a network of computers. Each transaction on the blockchain is grouped into a ’block’ and cryptographically chained to the previous one, forging an immutable audit trail [36].

Smart contracts, a feature of several blockchain platforms, are self-executing code residing on the blockchain. They enforce contract terms triggered by predefined conditions, such as the receipt of an RFID-tagged asset [37]. When integrated with RFID, smart contracts pave the way for trustless and automated ownership transfers. Key suitability aspects include:

- Decentralisation: Eliminating central intermediaries through blockchain decentralisation mitigates bottlenecks and single points of failure, bolstering the scalability and resilience of RFID-based ownership management systems.
- Security and Immutability: Blockchain’s inherent cryptographic functions secure ownership data, making it resistant to tampering. Any attempts to alter records create inconsistencies that the network flags, enhancing trustworthiness.
- Automation: Smart contracts automate ownership updates when associated RFID tags trigger predefined conditions, minimising manual intervention and associated delays or errors. This streamlines supply chain operations, improving overall efficiency.
- Transparency: Blockchain’s distributed ledger offers a shared, immutable view of ownership data across multiple stakeholders in the supply chain. This visibility reinforces trust and promotes proactive conflict resolution.

While there are ongoing technical challenges with blockchain scalability and energy use, exploring this technology presents exciting potential for the realisation of decentralised RFID ownership transfer systems that address the limitations of traditional architecture.

5.3.4. CO-TSM-Based Smart Supply Chain

The integration of the Consumer-Oriented Trusted Service Manager (CO-TSM) within smart supply chains ushers in a paradigm shift in how RFID ownership and the associated data management are approached. At its essence, CO-TSM leverages the robustness of blockchain technology to facilitate a secure, transparent, and decentralised framework for managing the lifecycle of RFID tags from production through to end-user handling. This section will explore the foundational concepts of CO-TSM, its integration with RFID technology, and the pivotal role of smart contracts in orchestrating ownership transfer seamlessly across the supply chain.

Detailed Operational Walkthrough is list below and illustrated in Figure 13.

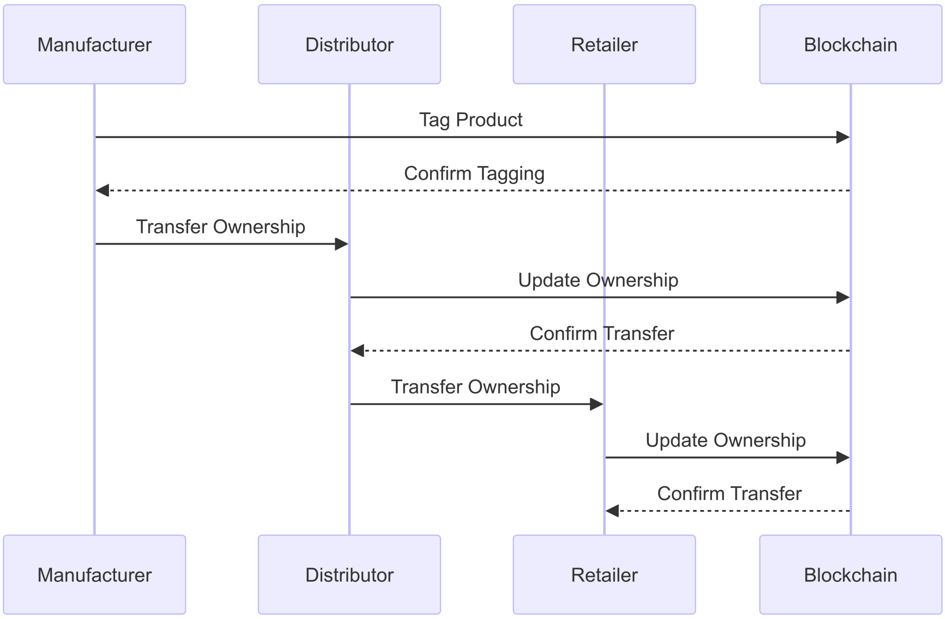


Figure 13. Sequence diagram illustrating the ownership transfer process in a CO-TSM-based smart supply chain.

1. Step 1: Initialisation and Tagging: The journey begins with the tagging of physical products with RFID tags. Each tag is encoded with unique identifiers that link to a digital twin on the blockchain. This digital twin houses essential information about the product, including its provenance, current ownership, and transaction history.
2. Step 2: Ownership Transfer Mechanism: As products traverse through various stages of the supply chain, their ownership status is poised for transfer. The smart contracts, designed with pre-defined rules for ownership transfer, play a critical role here. They automatically execute upon the fulfilment of specified conditions, such as a sale or consignment agreement, thereby initiating the ownership transfer process on the blockchain.
3. Step 3: Smart Contract Execution: Upon activation, the smart contract verifies the transaction against its conditions, ensuring all criteria are met for a legitimate transfer. It then updates the blockchain ledger, reflecting the new ownership of the RFID tag. This process is immutable and transparent, providing an incontrovertible record of the transaction.
4. Step 4: Notification and Verification: Stakeholders involved in the transaction receive notifications of the ownership change. They can independently verify the updated ownership status through the blockchain, ensuring transparency and trust among parties.

In-depth Analysis of System Benefits

The CO-TSM-based smart supply chain framework brings forth a multitude of benefits, addressing several longstanding challenges in supply chain management.

1. Enhanced Security and Immutability: By leveraging blockchain's inherent security features, the system ensures that all transactions are secure and immutable, significantly reducing the risk of fraud and tampering.
2. Decentralisation and Trust: The decentralised nature of blockchain eliminates reliance on central authorities, fostering a trustless environment where transactions are verified by consensus.
3. Efficiency and Reduction of Errors: Automation through smart contracts minimises manual handling, streamlining operations, and reducing the likelihood of errors.
4. Transparency and Traceability: The system provides unparalleled transparency, allowing stakeholders to trace the history and ownership of products in real-time.

While the CO-TSM-based smart supply chain presents a different approach, it is not without challenges. Scalability, the energy consumption of blockchain networks, and the need for standardisation are areas that require further exploration. The section will conclude with a discussion on potential solutions and the future outlook of adopting CO-TSM in global supply chains.

The adoption of CO-TSM in RFID-enabled smart supply chains represents a significant leap forward in managing the complexities of modern supply chains. Through detailed explanations, operational walkthroughs, and a comprehensive analysis of benefits, this expanded section delves into the intricacies of CO-TSM and sets the stage for future innovations in supply chain management.

6. Limitations of the CO-TSM Model

Despite the numerous advantages and potential applications of the CO-TSM model, several limitations must be acknowledged. These limitations span technical, operational, and strategic domains and can influence the effectiveness and widespread adoption of CO-TSM in various industries, including HCE-TEE smartphones, IoT, and smart supply chains.

6.1. Technical Limitations

1. Scalability and Performance: The CO-TSM model introduces a decentralised architecture that requires robust key management and secure communication protocols. While this decentralisation enhances security and flexibility, it can also lead to scalability challenges, particularly in environments with a large number of devices. For instance, in smart supply chains, managing thousands of RFID tags and their associated cryptographic keys can become cumbersome. The overhead of secure communication and key management protocols may impact the performance of the system, especially in real-time applications. This is also evident in HCE-TEE smartphone deployments, where the increased battery consumption due to frequent secure communications and TEE operations can degrade the user experience.
2. Energy Consumption: Implementing CO-TSM in devices with limited power resources, such as IoT devices and RFID tags, can be challenging. The energy consumption associated with cryptographic operations and secure communications can significantly reduce the battery life of these devices. In the context of smart homes, where numerous IoT devices need to operate efficiently, the increased energy demands can strain the overall system and impact device longevity.
3. Interoperability Issues: The CO-TSM model aims to provide a flexible and user-centric approach to device management. However, achieving seamless interoperability between devices from different manufacturers and service providers remains a significant challenge. Different devices may use varying communication protocols, security standards, and TEE implementations, leading to compatibility issues. This is particularly evident in smart home environments, where diverse devices from multiple vendors need to work together harmoniously. In smart supply chains, the integration of RFID technology with existing systems requires overcoming interoperability barriers to ensure smooth operation across the supply network.

4. Complexity of Integration: Integrating the CO-TSM model into existing infrastructures can be complex and resource-intensive. Organisations may need to overhaul their current systems to accommodate the decentralised architecture and secure communication protocols of CO-TSM. This integration complexity can act as a barrier to adoption, especially for small and medium-sized enterprises with limited technical expertise and resources. In HCE-TEE smartphone deployments, the integration of TEE with existing mobile applications and infrastructure requires significant effort and coordination.

6.2. Operational Limitations

1. Management Overhead: The CO-TSM model decentralises the management of devices and applications, which can increase the operational overhead for service providers. Managing a distributed network of devices, ensuring secure key management, and handling updates and maintenance tasks require significant effort and resources. In smart supply chains, the continuous monitoring and updating of RFID tags across multiple stages of the supply chain can strain operational capabilities. Similarly, in smart home environments, the decentralised management of numerous IoT devices necessitates robust and efficient operational strategies.
2. Responsibility and Accountability: Decentralisation introduces ambiguity in responsibility and accountability. Determining which entity is responsible for security breaches, device malfunctions, or data integrity issues can be challenging. In traditional TSM models, a central authority assumes responsibility, but the CO-TSM model's decentralised nature necessitates clear agreements and accountability frameworks among stakeholders. This complexity is evident in the smart home case study, where multiple entities, including device manufacturers, service providers, and users, share responsibilities.

6.3. Strategic Limitations

1. Resistance to Change: Organisations accustomed to traditional centralised TSM models may resist adopting the CO-TSM model due to its fundamental shift in architecture and management practices. Convincing stakeholders of the benefits and addressing concerns related to decentralisation, security, and control requires substantial effort. This resistance is particularly pronounced in industries with established practices and long-standing relationships with central TSM providers. For example, in the smart supply chain industry, shifting to a decentralised CO-TSM model may face resistance due to entrenched centralised systems and practices.
2. Monopolistic Tendencies: The CO-TSM model aims to empower consumers and foster a competitive market environment. However, it does not address the behaviour of aggressive, non-cooperating entities that may seek to establish monopolies. These entities could selectively establish relationships with service providers, limiting consumer choice and undermining the model's flexibility. For instance, in the HCE-TEE smartphone deployment, a dominant service provider might restrict access to certain applications, thereby reducing the overall effectiveness of the CO-TSM model.

6.4. Case Study Insights and General Implications

The deployment of the Consumer-Oriented Trusted Service Manager (CO-TSM) model across various technological ecosystems—such as HCE-TEE smartphones, Internet of Things (IoT) environments, and RFID-enabled smart supply chains—yields significant insights into both the strengths and limitations of this model. These case studies highlight practical considerations that can inform future implementations and guide the ongoing development of CO-TSM architecture.

6.4.1. HCE-TEE Smartphone Deployments

In the context of Host Card Emulation (HCE) combined with Trusted Execution Environments (TEE) on smartphones, the integration of CO-TSM presents both opportunities and challenges. The CO-TSM enhances security by ensuring that critical operations, such as cryptographic processing and key management, are conducted within the secure bounds of the TEE, isolated from the general smartphone environment. This isolation significantly reduces the attack surface and protects sensitive information from potential breaches.

However, the integration of TEE with HCE is not without its drawbacks. One of the primary challenges is the impact on performance and energy consumption. The additional processing required for secure operations within the TEE can lead to slower response times and increased battery drain, which may adversely affect the user experience. As mobile devices continue to prioritise efficiency and user satisfaction, balancing security with performance remains a critical challenge for CO-TSM deployment in this space.

Moreover, the decentralised architecture that CO-TSM promotes requires robust and secure key management practices. Managing cryptographic keys across multiple service providers (SPs) and ensuring their secure distribution and storage is complex, particularly in a decentralised model where no single entity controls the entire process. Ensuring that keys remain secure while being accessible to authorised entities only adds to the technical challenges, necessitating innovative solutions in cryptographic key management.

6.4.2. IoT Deployments and Smart Home Environments

The deployment of CO-TSM within IoT ecosystems, particularly in smart home environments, brings to light the significant challenges of device diversity and protocol interoperability. The typical smart home consists of a wide range of devices—from security cameras and thermostats to smart lighting and appliances—each potentially operating on different communication protocols and standards. Integrating these devices into a unified, secure framework managed by CO-TSM requires addressing the lack of standardisation across devices and protocols.

Interoperability challenges extend beyond communication protocols to include the integration of different security standards and practices. Ensuring that all devices within a smart home network adhere to consistent security protocols while allowing them to communicate seamlessly is essential for maintaining the integrity of the network. CO-TSM must be capable of managing these diverse environments while enforcing security policies that protect users' data and privacy.

Additionally, the management overhead associated with maintaining a decentralised network of smart home devices poses a significant challenge for service providers. As the number of connected devices in a smart home grows, so does the complexity of managing security, updates, and user preferences. Service providers must develop efficient operational strategies to manage this complexity without compromising the user experience. This includes creating robust frameworks for accountability and responsibility, ensuring that each stakeholder—from device manufacturers to service providers—understands and fulfils their role in maintaining a secure smart home environment.

6.4.3. RFID-Enabled Smart Supply Chains

The integration of CO-TSM into RFID-enabled smart supply chains offers the potential to significantly enhance transparency, security, and efficiency within these complex networks. By leveraging CO-TSM, stakeholders in a supply chain can securely track and manage the flow of goods, ensuring that each transaction is recorded and verified in a decentralised manner. This capability is particularly valuable in industries where the authenticity and integrity of goods are critical, such as pharmaceuticals, luxury goods, and perishable items.

However, managing large-scale RFID networks presents its own set of challenges. The sheer volume of data generated by RFID tags, combined with the need for real-time processing and verification, can strain existing infrastructure. Ensuring the security of these transactions, especially when ownership of goods is transferred between entities, requires robust mechanisms for authentication, authorisation, and auditing. CO-TSM must facilitate these processes without introducing bottlenecks or vulnerabilities.

Moreover, the decentralised nature of CO-TSM necessitates clear accountability frameworks to manage responsibility among stakeholders. In a traditional, centralised supply chain, accountability is often easier to trace; however, in a decentralised model, it is crucial to clearly define roles and responsibilities to prevent disputes and ensure that each participant is held accountable for their actions. This includes managing the complexities of ownership transfer, where multiple parties may have a stake in the goods being transferred, each with different requirements for security and transparency.

6.4.4. General Implications for CO-TSM Adoption

The insights gained from these case studies underscore the need for careful consideration of both the technological and operational challenges associated with CO-TSM deployment. While the model offers significant benefits in terms of enhanced security, user control, and operational efficiency, its success depends on overcoming the inherent challenges in implementation.

From a technological standpoint, the primary concerns include ensuring that CO-TSM can operate efficiently without compromising performance, particularly in resource-constrained environments like smartphones and IoT devices. This requires ongoing research into optimising the performance of secure environments such as TEE and improving the efficiency of cryptographic operations.

Operationally, the adoption of CO-TSM demands collaboration between multiple stakeholders, including device manufacturers, service providers, and users. Establishing clear protocols for accountability, standardising communication and security protocols across devices, and educating users about their roles in maintaining security are all critical to the model's success.

In conclusion, while the CO-TSM model presents a promising approach to managing security and functionality in a decentralised ecosystem, its widespread adoption will require addressing both the technical and operational challenges highlighted by these case studies. Future research and development efforts should focus on optimising the model for different environments and creating frameworks that facilitate collaboration among stakeholders, ensuring that the benefits of CO-TSM can be fully realised across various applications.

6.4.5. Benefits of CO-TSM Adoption across Use Cases

The Table 3 summarises the key benefits that each of these use cases can realise by adopting the CO-TSM architecture:

This table highlights how CO-TSM can offer significant advantages across various technological ecosystems by enhancing security, increasing user control and flexibility, and improving operational efficiency. Each use case can leverage the decentralised and flexible nature of CO-TSM to overcome the limitations of traditional TSM models, thereby enabling more robust and adaptable management of secure applications and devices.

6.5. Future Research Directions

Addressing the limitations of the CO-TSM model requires ongoing research and development efforts. Future research should focus on:

- Improving Scalability: Developing efficient key management and communication protocols to enhance the scalability of CO-TSM in large networks of devices.
- Optimising Energy Consumption: Designing energy-efficient cryptographic operations and secure communication mechanisms to reduce the impact on battery life for IoT and RFID devices.
- Enhancing Interoperability: Standardising protocols and frameworks to ensure seamless interoperability between devices from different manufacturers and service providers.

- Simplifying Integration: Creating tools and methodologies to simplify the integration of CO-TSM into existing infrastructures, reducing the technical and resource barriers for adoption.
- Establishing Accountability: Developing clear accountability frameworks to manage responsibility and address security breaches, device malfunctions, and data integrity issues in decentralised environments.

In conclusion, while the CO-TSM model offers significant advantages in terms of security, flexibility, and consumer empowerment, it also faces several limitations that need to be addressed to achieve widespread adoption. By focusing on these areas, future research can further refine the CO-TSM model, making it a more robust and effective solution for secure embedded device management across various industries.

Table 3. Benefits of CO-TSM Adoption Across Different Use Cases.

Use Case	Enhanced Security	Increased User Control and Flexibility	Improved Operational Efficiency
HCE-TEE Smartphones	Secure isolation of critical operations within TEE; Reduced attack surface; Robust key management.	Users can switch CO-TSMs and install apps from any SP, providing flexibility.	Decentralised key management reduces dependency on a single entity, potentially lowering operational risks.
IoT/Smart Home	Consistent security protocols across diverse devices; Secure communication channels.	Users have control over device management and service providers, enhancing personalisation.	Efficient management of updates and security across numerous devices; Reduces complexity for service providers.
RFID-Enabled Smart Supply Chains	Decentralised verification of transactions; Enhanced traceability and accountability; Secure ownership transfers.	Enables stakeholders to manage their assets and transactions with greater autonomy.	Streamlined processes for tracking and managing goods; Real-time data processing without bottlenecks.

7. Conclusions and Key Takeaways

The Consumer-Oriented Trusted Service Manager (CO-TSM) model represents a significant evolution in the management of secure applications on NFC-enabled devices, multi-application smart cards, IoT devices, and RFID-based supply chains. Through its decentralised and flexible architecture, the CO-TSM model addresses many of the limitations inherent in traditional Trusted Service Manager (TSM) approaches, particularly in terms of scalability, user empowerment, and market fragmentation.

7.1. Key Contributions and Value to Knowledge

This paper makes several key contributions to the field of secure embedded device management:

1. Decentralisation of Application Management: The CO-TSM model decentralises the management of applications, allowing users and service providers greater autonomy and flexibility. This approach mitigates the centralised control bottlenecks that have historically plagued traditional TSM models.
2. Integration Across Technological Domains: By exploring the application of the CO-TSM model across various technological ecosystems—including HCE-TEE smartphones, IoT environments, and RFID-enabled smart supply chains—this paper demonstrates the model's versatility and adaptability. Each case study highlights the unique challenges and benefits associated with deploying CO-TSM in different contexts, offering valuable insights for future implementations.
3. Enhancement of Security Mechanisms: The CO-TSM model strengthens security by incorporating constant evaluation, remote attestation mechanisms, and robust key

management practices. These enhancements ensure that the security needs of modern, interconnected devices are met without compromising performance or user experience.

4. Addressing Market Fragmentation: By fostering greater interoperability and reducing reliance on centralised control, the CO-TSM model helps overcome market fragmentation issues. This allows for a more seamless integration of services across different platforms and devices, ultimately benefiting both service providers and consumers.
5. Identification of Challenges and Future Research Directions: The paper does not merely present the CO-TSM model as a solution; it also critically evaluates its limitations and identifies areas where further research and development are necessary. These insights provide a roadmap for advancing the CO-TSM model and ensuring its successful deployment in real-world scenarios.

7.2. Summary of Findings

The analysis and case studies presented in this paper underscore the following key takeaways:

- Scalability and Flexibility: The CO-TSM model's decentralised architecture provides a scalable solution for managing secure applications across a wide range of devices and platforms. This flexibility is particularly valuable in IoT and RFID environments, where the number of connected devices is continually growing.
- User Empowerment: By allowing users to choose and switch CO-TSMs and install applications from any service provider, the CO-TSM model empowers consumers with greater control over their devices. This user-centric approach aligns with the growing demand for personalised and adaptable technology solutions.
- Security and Trust: The CO-TSM model enhances security through continuous evaluation, remote attestation, and secure key management. These mechanisms help maintain the integrity of smart cards, IoT devices, and RFID systems, reducing the risk of breaches and ensuring that applications remain secure.
- Operational Challenges: While the CO-TSM model offers significant benefits, its implementation is not without challenges. Managing decentralised networks, ensuring interoperability between diverse devices, and overcoming resistance to change are critical areas that require careful consideration.
- Potential for Broad Application: The versatility of the CO-TSM model makes it applicable across various industries and technological domains. From enhancing the security of HCE-TEE smartphones to improving the efficiency of RFID-enabled supply chains, the CO-TSM model offers a robust framework for the future of secure embedded device management.

7.3. Future Outlook

The CO-TSM model, while promising, is still in its early stages of adoption. Future research should focus on overcoming the identified limitations, particularly in terms of scalability, energy consumption, interoperability, and integration complexity. Addressing these challenges will be crucial to the widespread adoption of CO-TSM across different industries.

Additionally, as new technologies emerge and the landscape of embedded devices continues to evolve, the CO-TSM model must adapt to meet these changes. Ongoing innovation in areas such as blockchain, AI-driven security, and advanced cryptographic techniques will likely play a pivotal role in shaping the future of CO-TSM and secure device management.

In conclusion, the CO-TSM model represents a significant advancement in the management of secure applications on embedded devices. By decentralising control, enhancing security, and empowering users, the CO-TSM model offers a compelling alternative to traditional TSM approaches. As the technology continues to mature, its potential to revolutionise the management of smart cards, IoT devices, and RFID systems will only increase, paving the way for a more secure and user-centric future in the realm of embedded device management.

Author Contributions: Conceptualization, K.M. and G.A.; methodology, K.M., G.A. and S.A.G.; software, C.S. and R.N.A.; validation, K.M., G.A., S.A.G., C.S., R.N.A. and D.S.; investigation, S.A.G. and C.S.; resources, R.N.A. and C.S.; writing—original draft preparation, K.M., G.A., S.A.G. and D.S.; writing—review and editing, K.M., G.A., S.A.G., C.S., R.N.A. and D.S.; visualization, K.M.; supervision, K.M. and D.S.; project administration, K.M.; funding acquisition, S.A.G. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Deanship of Research and Graduate Studies, King Khalid University, Grant number RGP1/349/45.

Data Availability Statement: Data are contained within the article.

Acknowledgments: The authors extend their appreciation to the Deanship of Research and Graduate Studies at King Khalid University for funding this work through small group research under grant number RGP1/349/45. All figures sourced from external publications are reproduced under the fair use doctrine for educational and academic purposes, with full attribution provided in the form "(Source: [Source Title + Citation])" in the figure caption, and complete details listed in the References section. The initial research, ideas, and draft of this paper were developed by the authors. To improve the language and communication, we utilised AI tools such as ChatGPT, Gemini, Claude, Grammarly and Quillbot. These tools helped refine the writing style and clarity of the paper. However, the core intellectual content, analysis, and contributions remain the work of the researchers.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Markantonakis, K. The Case for a Secure Multi-Application Smart Card Operating System. In *Information Security: First International Workshop, ISW'97, Tatsunokuchi, Ishikawa Japan, September 17–19. 1997, Proceedings*; Springer: Berlin/Heidelberg, Germany, 1998; pp. 188–197.
2. Girard, P. Which Security Policy for Multiplication Smart Cards? In Proceedings of the USENIX Workshop on Smartcard Technology on USENIX Workshop on Smartcard Technology, Berkeley, CA, USA, 10–11 May 1999; p. 3.
3. Chaumette, S.; Sauveron, D. Some Security Problems Raised by Open Multiapplication Smart Cards. In Proceedings of the 10th Nordic Workshop on Secure IT-Systems: NordSec 2005, Tartu, Estonia, 20–21 October 2005; Citeseer: Princeton, NJ, USA, 2005; pp. 20–21.
4. Foundation for Information Policy Research. *Framework for Smart Card Use in Government*; Technical Report; Foundation for Information Policy Research: Bedfordshire, UK, 1999.
5. Lindly, R.A. The Age of Smart Cards: An Exploratory Investigation of the Sociotechnical Factors Influencing Smart Card Innovation. Ph.D. Thesis, Department of Information and Communication Technology, Universtiy of Wollongong, Wollongong, NSW, Australia, 1996.
6. M'Chirgui, Z. The Economics of the Smart Card Industry: Towards Coopetitive Strategies. *Econ. Innov. New Technol.* **2005**, *14*, 455–477. [CrossRef]
7. NFCW. NFC Trials, Pilots, Tests and Live Services around the World. Technical Report. Available online: https://www.nfcw.com/list-of-nfc-trials-pilots-tests-and-commercial-services-around-the-world/ (accessed on 20 June 2024).
8. *Pay-Buy-Mobile: Business Opportunity Analysis*; White Paper 1.0; GSM Association: London, UK, 2007. Available online: http://www.gsmworld.com/documents/gsma_nfc_tech_guide_vs1.pdf (accessed on 20 June 2024).
9. Commerce, G.M. *The Role of the Trusted Service Manager in Mobile Commerce*; Technical Report; GSM Association: London, UK, 2013. Available online: http://www.gsma.com/digitalcommerce/wp-content/uploads/2013/12/GSMA-TSM-White-Paper-FINAL-DEC-2013.pdf (accessed on 20 June 2024).
10. *The Role and Scope of EMVCo in Standardising the Mobile Payments Infrastructure*; Technical Report; EMVCo.: Foster City, CA, USA, 2007.
11. *GlobalPlatform TEE Management Framework*; Technical Report v1.0; GlobalPlatform: Redwood City, CA, USA, 2016.
12. Alattar, M.; Achemlal, M. Host-Based Card Emulation: Development, Security, and Ecosystem Impact Analysis. In Proceedings of the 2014 IEEE International Conference on High Performance Computing and Communications, 6th IEEE International Symposium on Cyberspace Safety and Security, 11th IEEE International Conference on Embedded Software and Systems, HPCC/CSS/ICESS 2014, Paris, France, 20–22 August 2014; pp. 506–509. [CrossRef]
13. *Host Card Emulation (HCE) 101*; Whitepaper; A Smart Card Alliance Mobile & NFC Council: Redwood City, CA, USA, 2014. Available online: http://iqdevices.com/pdfFiles/HCE-101-WP-FINAL-081114-clean.pdf (accessed on 20 June 2024).
14. GlobalPlatform. Technical Report. 2016. Available online: https://www.globalplatform.org/ (accessed on 20 June 2024).
15. GlobalPlatform. *TEE System Architecture, Version 1.0*; GlobalPlatform Specifications; GlobalPlatform: Redwood City, CA, USA, 2011. Available online: https://www.globalplatform.org/specificationsdevice.asp (accessed on 20 June 2024).

16. *The Trusted Execution Environment: Delivering Enhanced Security at a Lower Cost to the Mobile Market*; Whitepaper; GlobalPlatform: Redwood City, CA, USA, 2015. Available online: http://www.globalplatform.org/documents/whitepapers/GlobalPlatform_TEE_Whitepaper_2015.pdf (accessed on 20 June 2024).
17. Statista. Arm's Market Share and Targets Across Key Technology Markets in 2019 and 2028 Fiscal Years. Technical Report. 2020. Available online: https://www.statista.com/statistics/1132112/arm-market-share-targets/ (accessed on 20 June 2024).
18. ARM Holdings. Record Shipments of Arm-Based Chips in Previous Quarter. Technical Report. 2020. Available online: https://www.arm.com/company/news/2020/02/record-shipments-of-arm-based-chips-in-previous-quarter (accessed on 20 June 2024).
19. Shepherd, C.; Arfaoui, G.; Gurulian, I.; Lee, R.P.; Markantonakis, K.; Akram, R.N.; Sauveron, D.; Conchon, E. Secure and trusted execution: Past, present, and future—A critical review in the context of the internet of things and cyber-physical systems. In Proceedings of the 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Tianjin, China, 23–26 August 2016; pp. 168–177.
20. Cerdeira, D.; Santos, N.; Fonseca, P.; Pinto, S. Sok: Understanding the prevailing security vulnerabilities in trustzone-assisted tee systems. In Proceedings of the IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 18–21 May 2020; pp. 1416–1432.
21. Shepherd, C. Techniques for Establishing Trust in Modern Constrained Sensing Platforms with Trusted Execution Environments. Ph.D. Thesis, Information Security Group, Royal Holloway, University of London, Egham, UK 2019.
22. Zheng, S.; Apthorpe, N.; Chetty, M.; Feamster, N. User perceptions of smart home IoT privacy. *Proc. ACM Hum.-Comput. Interact.* **2018**, *2*, 200. [CrossRef]
23. Albrecht, K.; Mcintyre, L. Privacy nightmare: When baby monitors go bad. *IEEE Technol. Soc. Mag.* **2015**, *34*, 14–19. [CrossRef]
24. Bastos, D.; Shackleton, M.; El-Moussa, F. Internet of Things: A survey of technologies and security risks in smart home and city environments. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT, London, UK, 28–29 March 2018. [CrossRef]
25. Smart Camera and Baby Monitor Warning Given by UK's Cyber-Defender. *BBC News*, 3 March 2020. Available online: https://www.bbc.co.uk/news/technology-51706631 (accessed on 20 June 2024).
26. Hackers Claim to Have Access to 50,000 Home Security Cameras. *Infosecurity Magazine*, 14 October 2020. Available online: https://www.infosecurity-magazine.com/news/hackers-access-50000-home-security/ (accessed on 20 June 2024).
27. Somebody's Watching: Hackers Breach Ring Home Security Cameras. *New York Times*, 15 December 2019. Available online: https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html (accessed on 20 June 2024).
28. Department for Digital, Culture, Media and Sport—UK Government. Code of Practice for Consumer IoT Security. Technical Report. 2018. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf (accessed on 20 June 2024).
29. Morgner, P.; Mai, C.; Koschate-Fischer, N.; Freiling, F.; Benenson, Z. Security update labels: Establishing economic incentives for security patching of IoT consumer products. In Proceedings of the IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 18–21 May 2020; pp. 429–446.
30. Noura, M.; Atiquzzaman, M.; Gaedke, M. Interoperability in internet of things: Taxonomies and open challenges. *Mob. Netw. Appl.* **2019**, *24*, 796–809. [CrossRef]
31. Costa, C.; Antonucci, F.; Pallottino, F.; Aguzzi, J.; Sarriá, D.; Menesatti, P. A review on agri-food supply chain traceability by means of RFID technology. *Food Bioprocess Technol.* **2013**, *6*, 353–366. [CrossRef]
32. Gupta, D.; Bhatt, S.; Gupta, M.; Tosun, A.S. Future Smart Connected Communities to Fight COVID-19 Outbreak. *Internet Things* **2021**, *13*, 100342. [CrossRef] [PubMed]
33. Fan, K.; Jiang, W.; Li, H.; Yang, Y. Lightweight RFID protocol for medical privacy protection in RFID-enabled healthcare environment. *IEEE/ACM Trans. Comput. Biol. Bioinform.* **2015**, *12*, 362–371.
34. Bottani, E.; Rizzi, A. Economical assessment of the impact of RFID technology and EPC system on the fast-moving consumer goods supply chain. *Int. J. Prod. Econ.* **2008**, *112*, 548–569. [CrossRef]
35. Chang, V.; Ramachandran, M.; Li, C.S.; Cruz, R.S. Blockchain-based trust management and authentication for distributed traceability in food supply chain. In Proceedings of the International Workshop on Security, Fukui, Japan, 2–4 September 2020; Springer: Cham, Switzeland, 2020; pp. 81–97.
36. Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Wen, Y.; Kim, D.I. A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access* **2019**, *7*, 22328–22370. [CrossRef]
37. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the internet of things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.