Where the POP Architecture Stands among the other RFID Solutions

K.H.S Sabaragamu Koralalage
Department of Information and Computer Sciences,
Saitama University, Saitama, 338-8570, Japan
krishan@gmail.com

Abstract

Radio frequency identification (RFID) is an emerging technology that is increasingly being used in business and industry, particularly in logistics, supply chain management and advanced applications. Their information storage capacity as well as their ability to transfer information through contact less means without line-of-sight creates significant advantage over other technologies. However, since those tags are bounded with constraints, with no foolproof method to manage the changing hands of the same-tagged item, and uncertainty in assuring of privacy and security in passive tags, none of the existing architecture or vender specific implementations could not solve this comprehensively by addressing the security risks and privacy threats arise in the domain of product lifecycle. Thus, there is a need to recognize a standard solution at least for a specific domain. Therefore we proposed the POP Architecture that comprehensively solves the problems arising in the domain of product lifecycle. In this paper, existing major solutions have been compared and distinguished against the POP architecture on protection against security attacks, privacy threats, and also with desired functionality of proposed solutions. Evaluation criteria have been provided, and then surveys of major proposed solutions, including ours are noted. Next, results of the evaluation are presented by addressing the security and privacy together with the functional aspects. Finally, the paper is concluded by realizing the best available solution for the product lifecycle with passive tags and discovering the position of POP architecture among them.

1. Introduction

Radio frequency identification (RFID) technology innovate many advanced applications as it allows decent information storage and contact less communication. It improves process automation efficiency and usability [8], allowing almost everything in the world to be uniquely numbered by embedding a RFID tag. However, it has become extremely difficult to protect the communication between the tags and the interrogators owing to the inherent constraints of the passive tags [1], and changing ownerships of the same-tagged products over the product lifecycle together creates security risks and privacy threats.

Constraints of the passive RFID tags can be classified into behaviors and characteristics. Behaviors of answering without the bearers' agreement, contact-less communication and large read range aggravate the risks while the characteristics like inability to be switched-off, to sense the reading and maintain a history of past readings or writings [8] also contribute to the same. Furthermore, as the tags are low in computational power, programmability and memory capacity, employing of strong security mechanisms are restricted [6,8].

Changing hands of the same-tagged products throughout the product lifecycle also exaggerates the problem [8]. As everybody involved in the product lifecycle need to share the

secrets, it is impossible to prevent illegal readings or writings. Therefore, predecessors' and successors' security and privacy are affected. On the other hand, unlike communication between computers, reverse engineering of RFID tags becomes an easy task. In addition to that, lacking methods to transfer the ownership, to allow multiple authorizations, to maintain long-term security, and to prevent anti-cloning of the tag considerably decreases the extensive use of RFID systems [1, 6, and 8].

The remainder of this paper is organized as follows: In Section 2, present the criteria to ensure the security and privacy with desired functional objectives on RFID solutions. Next, brief surveys of major solutions are provided in Section 3. The POP architecture [6] is described in Section 4. The Section 5 describes the evaluation results of those solutions against security and privacy criteria. Finally, those results were analyzed and found out where the POP architecture stands among other solutions, especially for the domain of product lifecycle.

2. Criteria for Security and Privacy

It is necessary to identify clear objectives when discussing security and privacy properties of various RFID designs. As the tags must not compromise the privacy or create any security risks to their holders. Information should not be leaked to unauthorized readers, nor should it be possible to build long-term tracking or associations between tags and holders. To prevent tracking, holders should be able to control the access to any tags they carry. Tag output should be distinguishable or easily modifiable to avoid long-term associations between tags and holders. Private information should not be stored inside the tag. Both tags and readers should trust each other. Spoofing either party should be difficult. Moreover, mutual authentication between tags and readers also provides a measure of trust. Focus should be given on session hijacking and replay attacks. Fault induction or power interruption should not compromise protocols. Resistant to replay or man-in-the-middle attacks is a must. To avoid such security risks and privacy threats, following objectives are derived. Thus it is possible to achieve the rigorous security and privacy in future RFID systems.

2.1. Security Objectives

The wireless communications between RFID transponders and readers yield a number of security issues. To eliminate security risks, fundamental information security objectives, such as confidentiality, integrity, availability, authentication, authorization, non-repudiation and anonymity [8] must be rigorously enforced. Therefore, comparison has been carried out based on those criteria plus achievement of forward security, anti-reverse engineering, and anti-cloning to check what level of security is provided by each of the above listed solutions. Each objective has basic conditions to fulfill and will be checked for four levels: fully satisfied, partially satisfied, not satisfied or not applicable.

2.2. Security Risks

As mentioned in the security objectives, if those objectives are achieved, following attacks can be alleviated. Attacks on tags/interrogators, Access-key or Cipher-text tracing, Eavesdropping, Spoofing, Man-in-the-Middle, Replay, Brute-force and Denial of Service will be evaluated by considering the fulfillment of the above security objectives. Each attack will be checked for full protection, partial protection and no protection by evaluating the achievement of the list of basic security objectives under each attack.

2.3. Privacy Objectives

Most personal privacy threats arise by the unique identity property of RFID tag, as it can be easily associated with an owner's identity. Therefore no private information or association should be stored inside the tag or they should be properly protected.

There are three main privacy objectives: provide protection against the leaking data or information, block off the tracing of behavior or location, and prevent identifying the owner or profiling. Each objective is checked and evaluated for the fulfillment as fully satisfied, partially satisfied, not satisfied and not applicable.

2.4. Privacy Threats

Privacy threats can be crucial to two parties: Corporate Privacy and Personal Privacy. Each party is vulnerable to specific threats. In addition to the security protection, each privacy objective should be achieved to protect the corporate privacy threats: Corporate espionage threat and Competitive marketing threat, and also the personal privacy threats: Action threat, Association threat, Location threat, Preference threat, Constellation threat, Transaction threat, and Breadcrumb threat [4]. Each threat is checked against the above privacy objectives and evaluated for the fulfillment as fully protected, partially protected, not protected and not applicable.

2.5. Functional Objectives

Functionality like, Interoperability, Reliability, Usability, Feasibility, Scalability, Ability to manage new and damaged tags, Control Accessing, Transfer ownership online or offline, Achieve multiple authorizations, and Recycling tagged products are checked for low, high and not applicable status.

3. Related Major Solutions

In this section, major solutions proposed so far to solve the security risks and privacy threats associated with the use of RFID systems are presented. Here the objective is not to give a detailed explanation of each solution, but to provide the reader with the fundamental principles. A critical review of every proposal and the bibliography can be checked in case someone wishes to deepen on some aspects of this subject. For simplicity, the existing major solutions have been divided into several categories as follows:

3.1. Device Added Schemes

3.1.1. Faraday Cage. A basic method to protect the privacy of objects labeled with RFID tags is by isolating them from any kind of electromagnetic waves [1]. This can be made using what is known as a Faraday Cage, a container made of metal mesh or foil that is impenetrable by radio signals at certain frequencies. The main problem here is that there will be infinite number of items that can not be shielded by Faraday cage while there is no assurance once it is uncovered.

3.1.2. Blocker Tag. Jules et al. [1] proposed the use of Blocker Tags to protect consumer privacy. A blocker tag spam unauthorized readers by manipulating the reading protocol to

make the reader think that RFID tags representing all possible serial numbers are present. When a Blocker Tag is in proximity to ordinary RFID tags, they benefit from its shielding behavior. When the Blocker tag is removed, the ordinary RFID tags may be used normally. The problem of blocker is that it cannot selectively block readers, that is, it cannot block rogue readers while at the same time allowing friendly readers to read the content of the tags. Also, it is inconvenient consumers to possess and carry a blocker tag in order to opt out of having their personal information leaked. For blocker tag approach, it adds a burden to consumers and also fails to protect consumers when products are separated from it.

3.1.3. RFID Guardian. RFID Guardian [10] is a device that allows people to administer the security of their RFID tags. It intermediates reader requests to tags and selectively simulates tags under its control. As a high powered device with substantive computing power, a Guardian can implement sophisticated privacy policies, and can use channels other than RFID to supplement ambient data. The problem here is that, it reduces the speed of communication and increases the cost, in addition to the burden of carrying an extra device.

3.2. Radio Frequency Modification Schemes

3.2.1. Reader Changes Frequency. Readers may employ random frequencies so that unauthorized users may not easily detect the traffic or perform eavesdropping [12].

3.2.2. Tag changes frequency. Specially designed tags can transmit signals over a reserved frequency indicating that they are being modified [12].

3.2.3. Antenna-energy analysis. This is a system based on the premise that legitimate readers are likely to be quite close to tags, whereas malicious readers are likely to be far away [12].

However, radio frequency modification approaches imply changing runtime radio frequency, which means complex circuits and hence the cost of building such a device will be high. As the cost of a tag is a crucial factor, the widespread adoption of a RFID solution in industry will then be limited.

3.3. Hash Based Schemes

One of the more widely used proposals to solve the security problems that arise from RFID technology is the use of hash functions.

3.3.1. Hash Lock. Weis [12,13] proposed a simple security scheme based on one-way hash functions. Each tag has a portion of memory reserved to store a temporary metaID and operates in either a locked or an unlocked state. The reader hashes a key k for each tag, and each tag holds a metaID (metaID = hash (k)). While locked, a tag answers all queries with this metaID and offers no other functionality. To unlock a tag, the owner queries the back-end database with the metaID from the tag, looks up the appropriate key and sends the key to the tag. The tag hashes the key and compares it to the stored metaID.

3.3.2. Randomized Hash Lock. One of the problems of the previous solution is that it allows the tracking of individuals. To avoid this, the metaID should be changed repeatedly in an unpredictable way. In order to solve this problem, Weis [13] proposed an extension of the hash lock scheme. It requires that tags have a hash function and a pseudo-random number generator [11].

3.3.3. Hash-Chain. Ohkubo, in [9], suggested a list of five points that must be satisfied in all security designs of RFID schemes: keep complete user privacy, eliminate the need for extraneous rewrites of the tag information, minimize the tag cost, eliminate the need for high power of computing units, and provide forward security. A hash-chain scheme was proposed, in which two hash functions (G and H) are embedded in the tag.

3.4. Pseudo Random Function Based Schemes

3.4.1. Scalable, Delegatable Pseudonym Protocol. Tags generate pseudonyms that can only be decoded with knowledge of the appropriate secrets, and privacy is protected by controlling which parties are given access to these secrets. The set of secrets are organized in a tree format and allows ownership transfer between users using trusted third party [7]. Though this scheme is practical and scalable, it yields a complexity and gives no control to the consumers after purchase. Similarly, the reading of an information tree is a time consuming task, which may affects the performance of the communication.

3.5. Re-encryption Schemes

3.5.1. Symmetric Key Encryption. Feldhofer [8] proposed an authentication mechanism based on a simple two-way challenge-response algorithm. The problem with this approach is that it requires having AES implemented in an RFID tag. In [11], we can find a state of the art on AES implementations in RFID systems.

3.5.2. Public Key Encryption. There are solutions that use public-key encryption, based on the cryptographic principle of re-encryption. The reader interested in the precise details can read the paper of Juels [2].

3.6. Other Solutions

3.6.1. Kill Command. This solution was proposed by the Auto-ID Center [1] and EPCglobal. In this scheme, each tag has a unique password, for example of 24 bits, which is programmed at the time of manufacture. Upon receiving the correct password, the tag will be deactivated forever. The kill tag approach is not a recommended solution. Many of RFID applications will require that tags still be active while in the consumer's possession, and thus cannot be killed upon purchase.

3.6.2. Zero-knowledge Device Authentication. Zero-knowledge protocols have been introduced with consumer control of keys to ensure consumer privacy needs by physical redesign of RFIDs [5]. According to this solution, no EPC Tag ID will be there in the Tag itself instead some other numbers, and also this solution does not provide the complete ownership transferring mechanism, therefore the problem can not be solved properly. Furthermore, no obvious method has been defined to control the security and privacy after purchase though they claim the solution facilitates ownership transference and multiple authorizations.

3.6.3. The Renaming Approach. Even if the identifier emitted by an RFID tag has no intrinsic meaning, it can still enable tracking. For this reason, merely encrypting a tag identifier does not solve the problem of privacy. An encrypted identifier is itself just a meta-identifier. It is static, and therefore subject to tracking like any other serial number. To prevent RFID-tag tracking, it is necessary that tag identifiers be suppressed, or that they change over time [3].

4. The POP Architecture

The POP architecture [6] is a mechanism used to ensure the security and privacy of the passive RFID systems used in a product lifecycle. It uses two techniques to achieve this goal. One is a tagged-product flow with an anonymous ownership transferring mechanism, and the other is a robust communicational protocol. The first point defines how the ownership should be transferred, how the product should flow over the product lifecycle by changing hands up to the point of recycling, and how to maintain the long term security. The latter is to read EPC to disable the tag, to change shared secrets, to change the authentication key, and to change the both shared secret and authentication key which means the ownership transference. Thus, the POP Architecture addresses the issues pertaining to tag constraints and changing hands of the same tag throughout the product lifecycle by using the two techniques mentioned above. Each technique solves several unique issues while both together solve the privacy issues.

Assuming that there is a proper radio-communication, the POP Architecture achieves several objectives. They are: working with the low budget, coping with the illegal reverse engineering, preventing the tag cloning and stop responding without bearer's agreement, maintaining long term security, eliminating the necessity of sharing secrets among each actors, keeping the province to disable a tag at any given time, managing multiple authorizations, and reusing tag through out the product lifecycle.

To maintain the long-term security, the two shared secrets used for trust establishment have to be changed in a periodical manner. This can also be called as forward security. This is practical only before the purchase. Higher the frequency of changing secrets, lower the risks. Yet there is a province to do the same after purchase, if consumers are provided with a writer or access to a writer. Similarly, the POP Architecture also allows consumers to change the PIN or the Card key in case of loosing the secrets. According to the EPC global and Alien Technology, recent developments in UHF tags are capable of writing minimum of 5 tags per second but expected to achieve 30 tags per second. This speed is slightly less than desired level to adopt POP Architecture efficiently. As a recommendation, to keep the higher security level, it is desired to update tags once in a month.

4.1 Risk Elimination by Protocol

By using the protocol used in POP architecture, several important security attacks can be prevented throughout the tagged-product's lifecycle. Following paragraphs explain how it is achieved.

Attacks on tags/interrogators (attacks, where attacker pretends to be as a valid interrogators) -As mutual authentication is done by using the generated nonce and two shared secrets, trust is established between the tag and the interrogator. Therefore, unauthorized interrogators can not act as a valid interrogator. Even if they try without appropriate shared secrets, tags will be silent and no impersonation is possible. Furthermore, encryption also

makes this extremely difficult. On the other hand, the ability of changing secrets periodically decreases the vulnerability of these attacks.

Access-key or Cipher-text tracing, Eavesdropping and Spoofing (Reading and recording the messages passed between tags and interrogators), and Man-in-the-Middle attack (Modifying the messages passed between tags and interrogators) -Tag output is indistinguishable from truly random values and un-linkable to EPC. On the other hand, the tag output is not constant and also it does not expose any meaningful information. Furthermore, as mutual authentication is done, two shared secrets are used, Grain1 [14] encryption algorithm with 80bits long key is used, and shared secrets are changed periodically, the above attacks will be extremely difficult.

Replay attack (Recording and reproducing the messages passed between tags and interrogators) -Since Interrogator generates nonce and sends it to the tag and tag also generates a nonce and sends that to the Interrogator, this attack is prevented.

Brute-force attack (Find out the encryption key of the algorithm and then attack) -Grain1 stream cipher algorithm [14] which uses 80bits long key and has the complexity of $O(2^{80})$ is used to reduce the possibility of brute force attack.

4.2 Anonymous Ownership Transferring Mechanism in Product Lifecycle

The POP Architecture defines the ownership by storing two secrets inside the tag. Transferring ownership means the changing of those secrets as shown in Fig.3. Since the stored secrets are in number format, it is not possible to recognize the owner. Therefore, this is called an anonymous ownership transferring mechanism. The methods of using those two secrets differ before and after purchase. Before purchase, those secrets act as authentication key and shared secret. Also the system will generate those secrets and feed them to the tag while keeping the records in a local database. Whereas after purchase, same secrets act as username and password which will be taken from swiping or proximity card key and PIN respectively. Unlike before purchase, no database records are maintained after purchase. Once the ownership is transferred, the predecessors can not read the tag as they are unable to provide new secrets that belong to successors. Basically these secrets act as a soft switch and help to cope with illegal tampering, prevents illegal reading, stop responding without bearer's consent, eliminate the necessity of sharing secrets, and manage multiple authorizations allowing the ownership transferring.

4.3 Risks Elimination by using Anonymous Ownership Transferring Mechanism

Ownership transferring mechanism in tagged-product facilitates reusing the same tag without any issue throughout the product lifecycle. Similarly, no need to share the secrets but each party will have to assign their own secrets to the own products by the time, they receive the products. Moreover, at any given time only one user owns the secrets and a user can grant the reading privilege only for one time read without revealing the stored secrets. In this way the multiple authorizations are managed.

Though there is no switch in a passive RFID tag, two shared secrets of POP Architecture will act as a protection switch; therefore no tag can be read without receiving the owner's approval. In other words no tag will respond without owner's permission.

Although the reverse engineering is uncontrollable, the above technique alleviates the risk magnitude in different capacity in these three scenarios. Firstly, buying the products from the retail store and reverse engineering; as after the purchase, stored secrets are changed to the customer's own secrets; attackers are unable to steal the stored secrets. Secondly, stealing the products before sales; as in each stage, secrets are different, and those secrets themselves are periodically changed, no one can attack the whole RFID system though they could access the stored secrets. Yet, if the attacker could reverse engineer the tag and attack before next update, damage will affect to one particular party. Finally, stealing products after sales; reverse engineering of the stolen products belonging to a customer could reveal the secrets of a specific customer. This can not be prevented by above technique. Even if the attacker finds out the stored secrets, only one customer can be attacked. On the other hand, attacker gets negligible merit in this stage. In case of such an attack, customers' are given the province to change the PIN, card key, and both to rebuild the security.

Cloning or forging of the tags becomes extremely difficult before purchase, as the tag secrets are changed periodically. Similarly cloning after purchase is also difficult as card key and PIN is used to establish the communication.

4.4 Privacy Threats Elimination using Both Techniques

Corporate and personal privacy threats are reduced using the two techniques written in section 4.2 and 4.3.

4.4.1. Corporate Privacy Threats. Corporate espionage threat and Competitive marketing threat can be reduced as tags will not response without the consent of the owner and no one has to share the secrets. Infrastructure facility threat can not be prevented by this method as it is over the control of the POP architecture.

4.4.2. Personal Privacy Threats. Action threat- If the store needs to monitor tagged product's movement and customer's action on that, it can not be prevented by the POP Architecture . If the attacker tries to monitor the bearer's action by reading the tagged-product, no threat will arise as they are unable to read the tag illegally.

Association threat- The POP Architecture will associate the owners anonymously, which makes it extremely difficult for an attacker to obtain the association. Also, protection against illegal reading prevents this threat.

Location threat, Preference threat, and Constellation threat- Since no tag responses without the bearer's agreement, no one can easily track the locations of the tagged-products or the bearer. Furthermore, the two shared secrets will prevent accessing the tag illegally.

Transaction threat- As there is a secured ownership transferring mechanism in each transaction, it is not easy to read or write illegally. Therefore, transaction threat will be avoided.

Breadcrumb threat- According to the POP Architecture, each item to be recycled will delete its two shared secrets which anonymously associate the owner and products. Therefore, no breadcrumb threat will occur as no fragment of them contains any association information when customer throws away the garbage.

5. Evaluation

Depending on the above criteria, proposed solutions are evaluated. When comparing against the security objectives (Table 1.), it is obvious that Active Jamming, Frequency modification, Kill Tag and Renaming

Table 1. Represents the fulfillment of security objectives before and after purchase [15]

Before Purchase / After Purchase — Security Objective	Faraday Cage[1]	Blocker Tag[1]	Active Jamming[1]	Frequency Modification[12]	Kill Tag[1]	RFID Gardian[10]	Renaming[3]	Hash Based Schemes[12],[11],[9]	Delegated Psudonym[7]	Zero knowledge[5]	Re-encryption [8],[2]	POP Architecture[6]
Authentication	NS / NS	NS / NS	NS / NS	NS / NS	NS / NA	PS / PS	NS / NS	PS / PS	PS / PS	PS / PS	PS / PS	FS / FS
Authorization	NS / NS	PS / PS	NS / NS	NS / NS	NS / NA	PS / PS	NS / NS	PS / PS	PS / PS	FS / FS	PS / PS	FS / FS
Confidentiality	PS / PS	PS / NS	PS / NS	PS / NS	NS / NA	PS / PS	NS / NS	PS / PS	PS / PS	FS / FS	PS / PS	FS / FS
Anonymity	NS / NS	PS / NS	NS / NS	PS / NS	NS / NA	NS / NS	PS / PS	PS / PS	PS / PS	PS / PS	PS / PS	FS / FS
Data Integrity	NS / NS	NS / NS	NS / NS	NS / NS	NS / NA	PS / PS	NS / NS	PS / PS	PS / PS	PS / PS	PS / PS	FS / PS
No-Repudiation	NS / NS	NS / NS	NS / NS	NS / NS	NS / NA	NS / NS	NS / NS	NS / NS	NS / NS	PS / PS	NS / NS	FS / FS
Availability	PS / PS	NS / NS	NS / NS	NS / NS	NS / NA	PS / PS	NS / NS	PS / PS	PS / PS	PS / PS	PS / PS	PS / PS
Forward Security	NS / NS	NS / NS	NS / NS	NS / NS	PS / NA	NS / NS	NS / NS	PS / PS	PS / PS	FS / PS	PS / NS	FS / PS
Anti-Cloning	NS / NS	PS / NS	NS / NS	NS / NS	NS / NA	NS / NS	NS / NS	PS / NS	PS / PS	FS / PS	PS / NS	FS / PS
Anti-Reverse Engineering	NS / NS	PS / NS	NS / NS	NS / NS	NS / NA	NS / NS	NS / NS	PS / NS	NS / NS	FS / PS	PS / NS	FS / PS

Partially Satisfied -PS Fully Satisfied -FS Not Satisfied -NS Not Applicable -NA

Table 2. Represents the protection against security attacks before and after purchase [15]

Before Purchase / After Purchase — Security Attack	Faraday Cage[1]	Blocker Tag[1]	Active Jamming[1]	Frequency Modification[12]	Kill Tag[1]	RFID Gardian[10]	Renaming[3]	Hash Based Schemes[12],[11],[9]	Delegated Psudonym[7]	Zero knowledge[5]	Re-encryption [8],[2]	POP Method[6]
Attacking RFID Tags	FP / FP	PP / PP	NP / NP	NP / NP	NP / PP	PP / PP	NP / NP	PP / PP	PP / PP	FP / P	FP / PP	FP / FP
Attacking Interrogators	NP / NP	PP / PP	NP / NP	NP / NP	NP / NA	PP / PP	NP / NP	PP / PP	PP / PP	FP / P	PP / PP	PP / PP
Access-key/Cipher-text Tracing	NP / NP	PP / PP	NA / NA	NA / NA	NP / NA	PP / PP	NA / NP	PP / PP	PP / PP	PP / P	FP / PP	FP / PP
Eavesdropping	NP / NP	PP / PP	NP / NP	PP / NA	NP / NA	PP / PP	NP / NP	PP / PP	PP / PP	PP / P	FP / PP	FP / PP
Spoofing	NP / NP	PP / PP	NP / NP	PP / NA	NP / NA	PP / PP	NP / NP	PP / PP	PP / PP	PP / P	FP / PP	FP / PP
Man-in-the-middle	NP / NP	PP / PP	NP / NP	NP / NA	NP / NA	PP / PP	NP / NP	PP / PP	PP / PP	PP / P	FP / PP	FP / PP
Replay Attack	NP / NP	PP / PP	NP / NP	NP / NA	NP / NA	PP / PP	NP / NP	PP / PP	PP / PP	PP / P	FP / PP	FP / PP
Brute-force Attacks	NA / NA	PP / PP	NP / NP	NA / NA	NA / NA	PP / PP	NA / NA	PP / PP	PP / PP	PP / P	PP / PP	PP / PP

Fully Protected -FP Partially Protected -PP Not Protected -NP Not Applicable -NA

are well below the required level whereas Faraday cage, blocker tag and RFID Guardian achieve several objectives than them. Yet, they are also below the desired level when Hash based Schemes, Delegated Pseudonym Protocol, Zero knowledge, re-encryption methods, and POP Architecture are considered. On the other hand, Zero knowledge and POP show the confidence in all the objectives. However, after taking a closer look, One could identify that the POP Architecture is little stronger than the Zero knowledge scheme as it supports secure usage even after purchase. When attack analyses (Table 2) are considered, It was possible to recognize that the Blocker tag, RFID guardian, Hash based schemes, Delegated pseudonym, Zero knowledge, Re-encryption and POP are well above the average but only the Re-encryption and POP Architecture provides a considerable protection against those security attacks. Privacy Protection (Table 3) shows that only the Kill tag, Re-encryption and POP Architecture protect the privacy considerably whereas the POP Architecture achieves the optimum privacy. As far as Functional analysis (Table 4) is considered, the ability of POP Architecture is well beyond the all other solutions available for comparison.

Table 3. Represents the corporate and personal privacy protection [15]

Corporate Privacy Protection	Faraday Cage[1]	Blocker Tag[1]	Active Jamming[1]	Frequency Modification[12]	Kill Tag[1]	RFID Gardian[10]	Renaming[3]	Hash Based Schemes[12],[11],[9]	Delegated Psudonym[7]	Zero knowledge[5]	Re-encryption [8],[2]	POP Method[6]
Corporate espionage threat protection	PP	PP	NP	PP	NP	PP	NP	PP	PP	PP	PP	FP
Competitive marketing threat protection	PP	PP	NP	PP	NP	PP	NP	PP	PP	PP	PP	FP
Personal Privacy Protection												
Action threat protection	PP	PP	NP	PP	FP	PP	NP	PP	PP	PP	FP	FP
Association threat protection	PP	PP	NP	PP	FP	PP	NP	PP	PP	PP	FP	FP
Location threat protection	PP	PP	NP	PP	FP	PP	NP	PP	PP	PP	FP	FP
Preference threat protection	PP	PP	NP	PP	FP	PP	NP	PP	PP	PP	FP	FP
Constellation threat protection	PP	PP	NP	PP	FP	PP	NP	PP	PP	PP	FP	FP
Transaction threat protection	PP	PP	NP	PP	FP	PP	NP	PP	PP	PP	FP	FP
Breadcrumb threat protection	NP	PP	NP	PP	NP	NP	NP	NP	NP	NP	NP	FP

Fully Protected -FP Partially Protected -PP Not Protected -NP Not Applicable -NA

Although security objectives (Table 1) and attack analysis (Table 2) reveal that Delegated pseudonym protocol, Zero-knowledge, Hash based schemes, Re-encryption and POP Architecture are above the average of security risks prevention, privacy threat analysis (Table 3) and functional analysis (Table 4) reveal that no solution other than POP Architecture provides a way to transfer ownership online or offline, enables method to achieve multiple authorizations, and allows user to control communication.

When considering the post purchase usage, protection of personal privacy is a must. After carefully deriving results from the comparison, it is revealed that POP Architecture protects the personal privacy and corporate privacy not only in several phases but also in the transition stage. Thus, out of all the solutions, POP Architecture satisfies almost all the requirements though the tag has to be redesigned while it entails little more resource requirements. In contrast to previous proposals, we believe that redesigning of the tag structure by enabling POP Architecture to be used in RFID environment will solve the general fears and enable novel ubiquitous applications in near future.

Table 4. Represents the functional ability of each solution before and after purchase [15]

Ability (Before Purchase / After Purchase)	Faraday Cage[1]	Blocker Tag[1]	Active Jamming[1]	Frequency Modification[12]	Kill Tag[1]	RFID Gardian[10]	Renaming[3]	Hash Based Scheme[12],[11],[9]	Delegated Psudonym[7]	Zero knowledge[5]	Re-encryption [8],[2]	POP Method[6]
Interoperability	L / L	L / L	L / L	L / L	L / NA	L / L	L / L	L / L	L / L	L / L	L / L	H / H
Reliability	H / H	L / L	L / L	L / L	H / NA	L / L	L / L	L / L	H / L	H / L	H / L	H / L
Usability	L / L	H / H	NA / NA	NA / NA	H / NA	L / L	L / L	L / L	L / L	H / L	H / L	H / L
Feasibility	L / L	H / H	L / NA	L / NA	H / NA	L / L	L / L	L / L	L / L	H / H	H / H	H / H
Scalability	L / L	L / L	NA / NA	NA / NA	H / NA	L / L	H / H	L / L	L / L	H / L	H / H	H / H
Manage new and damaged tags	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	H / H
Control Accessing	H / H	H / L	NA / NA	L / NA	NA / NA	H / H	NA / NA	NA / NA	NA / NA	L / NA	NA / NA	H / H
Transfer ownership online/offline	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	L / L	L / NA	NA / NA	H / H
Achieve multiple authorizations	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	H / H
Recycle the tagged products	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	NA / NA	H / H

High -H Low -L Not Applicable -NA

6. Concluding Remarks

As the POP architecture prevents both risks arising within the communication system and the changing hands of the same tag throughout the product lifecycle, evaluation result reveals that it is the best available solution to address security and privacy issues for individuals and corporations from the point of production to recycling. Reason for that conclusion includes, POP architecture's ability of preventing security attacks, ability of ensuring privacy, and rate of interoperability, level of feasibility, scalability, manageability of new and damaged tags, self controllability, capability of resolving multiple authorizations and also ability of transferring ownership anonymously either online or offline throughout the product lifecycle.

Though it is necessary to redesign the tag with little more resources, and yields a universal customer card with PIN number to enable communication between tagged products after purchase, the position of POP architecture was clearly visible among the existing major solutions and found that no solution provides such level of achievement so far.

As future works, we hope to conduct more experiments to see the storage, computation and performance overheads of the POP architecture to provide a solid solution to answer the general uncertainties on RFID usage.

7. References

[1] A. Juels, R. Rivest, and M. Szydlo, "The blocker tag: Selective blocking of RFID tags for consumer privacy", *ACM CCS*, ACM Press, USA, 2003, pp. 103–111.

[2] A. Juels and R. Pappu, "Squealing euros: Privacy protection in RFID-enabled banknotes". *In Proc. FC'03*, LNCS 2742, January 2003, pp. 103-121.

[3] A. Juels, "RFID Security and Privacy: A Research Survey", *J-SAC*, 2006.

[4] A. Juels, R. Pappu, and S. Garfinkel. "RFID Privacy: An Overview of Problems and Proposed Solutions", *In Proc. IEEE Security and Privacy*, May/June 2005, pp. 34-43.

[5] S. Engberg, M. Harning, D. Jensen, "Zero-knowledge Device Authentication: Privacy and Security Enhanced RFID", *In Proc. Conference on Privacy, Security and Trust*, Canada, 2004, pp. 89-101.

[6] K. H. S. S. Koralalage, M. R. Selim, J. Miura, Y. Goto, and J. Cheng, "POP Method: An Approach to Enhance the Security and Privacy of RFID Systems Used in Product Lifecycle with an Anonymous Ownership Transferring Mechanism", *In Proc. SAC*, ACM Press, 2007, pp. 270-275.

[7] M. David, S. Andrea, and W. David, "A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags", LNCS 3897, 2006, pp 276-290.

[8] M. Feldhofer, S. Dominikus, and J.Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm". *In Proc.CHES*, LNCS 3156, 2004, pp. 357-370.

[9] M Ohkubo, K. Suzuki, and S Kinoshita, "Cryptographic approach to privacy friendly tags", *In Proc. RFID Privacy Workshop*, 2003.

[10] M. Rieback, B. Crispo, and A. Tanenbaum. "RFID guardian: A battery-powered mobile device for RFID privacy management", *In Proc. ACISP*, LNCS 3574, 2005 pp. 184–194.

[11] P.L Pedro, J. Cesar H.C., Juan E.T, and Arturo R., "RFID systems: A survey on security threats and proposed solutions", *In Proc. IFIP PWC*, LNCS 4217, 2006, pp. 159–170.

[12] Z. Luo, T. Chan, Jenny S. Li, "Lightweight Mutual Authentication Protocol for RFID Networks", *In Proc. IEEE ICEBE*, 2005 pp.620 - 625

[13] S.A Weis, S.E Sarma, R.L Rivest, and D.W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", *In Proc. Security in Pervasive Comp*, LNCS 2802, 2004pp. 201-212.

[14] H Martin, J Thomas and M. Willi, "Grain -A Stream Cipher for Constrained Environments", *In Proc. ECRYPT Workshop*, 2005, pp. 114-125.

[15] K. H. S. Sabaragamu Koralalage and Jingde Cheng "A Comparative Study of RFID Solutions for Security and Privacy: POP vs. Previous Solutions", Proceedings of the 2nd International Conference on Information Security and Assurance (ISA '08), pp. 342-349, Busan, Korea, IEEE Computer Society Press, April 2008.

Author

K.H.S Sabaragamu Koralalage is pursuing PhD in the Dept. of Information and Computer Sciences of Saitama University Japan. He achieved the MBCS in 2003 and received the MSc. Degree from International University of Japan in 2004. His main interest includes security and privacy issues in RFID, Ubiquitous RFID application development, Mobile RFID systems and sensor networks. He designed a novel architecture called POP, for passive RFID tags used throughout the product lifecycle.