Applying EPCglobal Architecture Framework for Criminal Physical Evidence Safety Monitoring System*

Chia-Chun Chen and Chua-Huang Huang
Department of Information Engineering and Computer Science
Feng Chia University
{georgechen, chh}@rfidlab.iecs.fcu.edu.tw

摘要

目前，證據保存的方法是執法人員於證據的取得、交接、保管時在交接物證清單上簽名，以確認物證保管的連續性、物證辨識及其狀態的完整性，讓證據能充份受到保護。但保管人無法確保在保管期間，對物證隨時進行安全控管，容易造成管理上弊端。本研究不再以保管人簽名程序為鏈的方式，來確保物證監管鏈是否出現斷裂的情形，而是以物證的角度加入 RFID 技術來確保物證監管鏈的完整性。我們以 EPCglobal 基礎架構來設計物證監管鏈系統，此系統著重在物證封緘袋結合 RFID 標籤的編碼設計與贓物庫內物證監控情境。我們對物證監管鏈所產生的事件加以定義，並儲存到 EPCIS 事件庫。同時，分析比對出系統所需要的事件，即時將物證的異常狀況回報給承辦人員，隨時確保物證監管鏈的完整性。此系統使得物證的交接流程、保存期間、及有異常狀況時具有追溯性，讓物證能實現更智慧化的管理，以提升物證保管業務的執行效能。

關鍵詞：證物監管鏈、EPCglobal 架構、無線射頻辨識、電子產品代碼資訊服務、複合事件處理

ABSTRACT

Currently, continuous preservation of evidence is based on a list of signatures which are signed at the time when law enforcement officers obtain, transfer, and store evidences. With signature process, it is possible to protect the continuity of custody of evidence, evidence identification, and integrity of the state. However, it can hardly ensure the evidence is under security control at any time, i.e., it may cause serious flaws by carelessly and/or intentionally breaking the custodian chain. In this paper, we do not only rely on custodian signature chain, but we also employ RFID technology to ensure the integrity of the chain of custody evidence. Based on EPCglobal architecture framework, we focus on evidence sealed bags which are affixed with RFID tags and monitor all events on evidences at any time. The chain of evidence custody becomes a sequence of events which are captured and stored in the EPCIS event repository. Meanwhile, the system analyzes and compares events needed to instantly detect abnormal conditions and sends messages to related personnel at any time to ensure the integrity of the chain of evidence custody. This system provides traceability of evidence during the period of transferring and preserving evidence with abnormal conditions. As a result, the chain of evidence custody can be more intelligent and efficient.

Keywords: chain of evdience custody, EPCglobal Architecture Framework, radio frequency identification, EPC Information Service, complex event processing

I. INTRODUCTION

Chain of custody is defined as an evidence control procedure to describe how to collect, packet, transport, transfer, and store evidence starting from crime scene until completing trial in the court [11]. An evidence control procedure is to ensure that evidence is handled under the supervision of law enforcement officers with detailed recording, packaging, sealing, preserving, and identifying until it is transferred to the court. All of these steps are authorized and verified by signatures of individuals who get involvement during the entire course of the chain of custody [1].

With signature procedure, it is possible to protect the continuity of custody of evidence, evidence identification, and integrity of the state. However, how to maintain the chain unbroken in the transferred process is a challenge for each individual. The law enforcement officers must precisely document and monitor the location and physical status of evidence; otherwise, the custodian system would not be able to effectively and efficiently maintain the integrity, accountability, and continuity of storage of physical evidences. Once the chain of evidence custody is broken, it may result in the inadmissibility of the evidence and diminishing the value of evidence in the court.

In this paper, our goal is to utilize RFID technology to enhance safety and integrity of the chain of evidence custody. We present a monitoring system of custodian evidences based on EPCglobal Architecture Framework [14] and complex event processing to design and implement chain of evidence custody [2, 10, 16]. The focus is on evidence sealed bags which are affixed with RFID

* This work was supported in part by National Science Foundation, Taiwan, under grant NSC 102-2218-E-035-006.

tags and monitor all events taking place on tags at any time. The chain of evidence custody then becomes a sequence of simple events which are captured and stored in the EPCIS event repository [5].

Simple events captured form an event stream which arrives to the system. In addition, a group of relevant simple

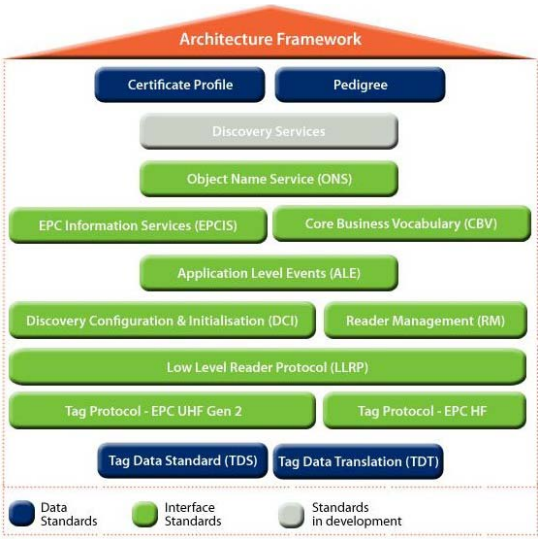

Figure 1. EPCglobal Architecture Framework (source: GS1, EPCglobal)

events is composed as a complex event is specified by a complex event rule [15]. Complex event rules are expressed using SQL-like statement and can be executed to analyze and trigger other events [8, 9].

The monitoring system of chain of evidence custody will capture EPCIS events and analyze these events according complex event rules to detect abnormal conditions such as unauthorized access to the evidence and missing evidence in real time. Once an abnormal condition is detected, a warning message and/or alarm will be issued to related personnel. Furthermore, this system provides track and trace capability of events that allow law enforcement office to investigate flaws of evidence custody.

This paper is organized as the followings. The next section gives a brief overview of EPCglobal Architecture Framework. We present the physical evidence safety monitoring system in Section II. The implementation using a Class-1 Generation-2 reader/tag simulator is explained in Section IV. Section V is the conclusion and future works.

II. EPCGLOBAL ARCHITCTURE FRAMEWORK

EPCglobal Architecture Framework is proposed by GS1 that utilizes RFID technology and supports global supply chain management [14]. The architecture framework includes 14 standard specifications and is divided into three layers: identify layer, capture layer, and exchange layer as shown in Figure 1.

1) Identify layer: This layer mainly defines the air interface and communication protocol between RFID readers and tags. Both high frequency (13.56 MHz) and ultra-high frequency (860 to 960 MHz) technologies are defined as Class-1 HF and Class-1 Generation-2 UHF tag protocol. In addition, Tag Data Standard (TDS) and Tag Data Translation (TDT) specify electronic product code (EPC) coding schemes and conversion between EPC and bar code [6].

In the chain of evidence custody we will employ the coding scheme to defne types of EPC code to identify evidence items, evidence packages, persons, and locations involed in the chain. The code is stored in an RFID tag and it can be read by readers to identify corresponding objects, persons, and locations.

2) Capture layer: The core in the capture layer is a middleware system specified as Application Level Events (ALE) [3]. The functions of the ALE middleware is to filter and aggregate tag data read by readers and to send them to capture programs.

In chian of evidence custody, readers may behave differently according to their nedds. Readers for monitoring evidence storage room may be activated in certain period of time, e.g, every 15 minutes; readers at the door entrace may be activated when an infrared sensor detects approaching object; readers in the court may be activated manually when evidence of inspected. The ALE middleware supports three methods of event cycle specifications (ECSpec) to control reader hehaviors, i.e., subscribe, poll, and immediate. With these three methods, we can make the readers in chain of evidence custody function properly as the monitoring system is carried on.

3) Exchange layer: Tag data are stored and retrived in the exchange layer. The main system is EPC Information Service (EPCIS) [5]. Basically, EPCIS is a database which stores tag data as events. An event is composed of four attributes: EPC list denoting the objects being captured, event time denoting the time when tag data are captured, record time denoting the time when the event is recorded, and reader point denoting the location where the event taking place. In addtion, a set of master data is specified in Core Business Vocabular (CBV) to express actions about the event [4]. EPCIS defines four types of events: object event type, aggregation event, quantity event type, and transaction event type. Upon receiving tag data in event cycle reports (ECReport) from the ALE middleware, capture applications will generate relevant event attribute values to create EPCIS events and store them in EPCIS event repository. In

the mean time, capture applications will forward EPCIS events to the complex event processing engine to performe context aware analysis specified by complex event rules. When performing complex event processing, the engine may query EPCIS to retrieve past relevant events.

The evidence safty mornitorng system will define its vocabularies and modify master data table for the proper usage in the chain of evidence custody. We will design a set of capture applications and complex event rules to implement chain of evidence custody.

III. Chain of Evidence Custody

In this section, we begin with description of vocabulary master data for chain of evidence custody. Then, explain the coding scheme of tag identification in chain of evidence custody and security mechanism for evidence bags. Finally, we use the store room as an example to illustrate the monitoring system.

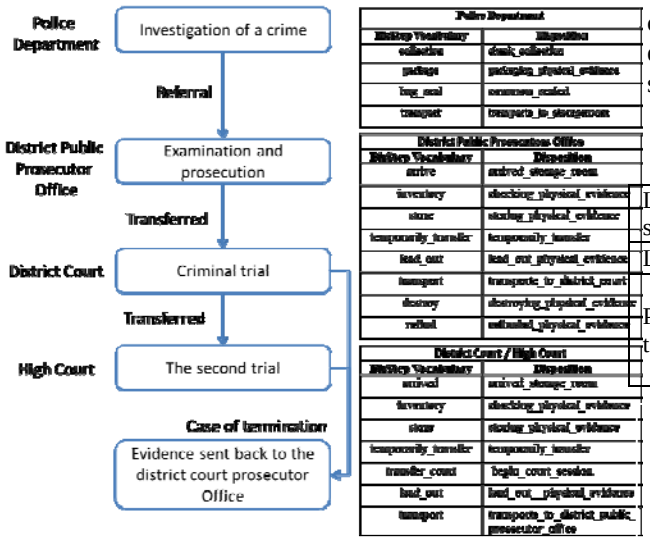

Figure 2. Vocabulary master data

A. Vocabulary Master Data

EPCglobal Architecture Framework is developed for global supply chain management and CBV is defined for business scenarios. For the chain of evidence custody, we redefine the vocabulary master data to record actions and states of the crime detection and processing procedure.

The crime detection and processing procedure starts at the crime scene where physical evidences are collected by police. The physical evidences are stored at the district court prosecutor office. During trials, the physical evidences are transport to the courts [12, 13].

The vocabulary master data are redefined according to the location where the physical may be collected, stored, transferred, and inspected as in Figure 2. The vocabularies for actions are collection, package, bag_seal, transport, arrive, inventory, store, temporarily_transfer, lead_out, destroy, and refind. These are actions may take place when process physical evidences. For each action, we use the following words to describe its disposition state such as check_collection, packaging_physical_evidence, common_ sealed, transporte_to_storage_room, arrived_storage_ room, checking_physical_evidence, storing_physical_ evidence, temporarily_transfer, lead_out_physical_ evidence, transporte_to_district_court, *etc*. These vocabularies may be extended when necessary.

B. Tag Coding

We will attach C-1 Gen-2 tags on each physical evidence item, evidence bags, and personnel who have contact with the evidence. For the identification purpose, tag identification must be coded according to the process of the chain of evidence custody and we will define the EPC coding scheme to fit into EPCglobal TDS specification.

Table 1. EPC Encoding Format

Logical segment	Company prefix	Item reference	Serial number
Length	27 bits	17 bits	38 bits
Partition table	country code (3 digits) + authority code (5 digits)	year (3 digits) + case number (2 digits)	serial number (12 digits)

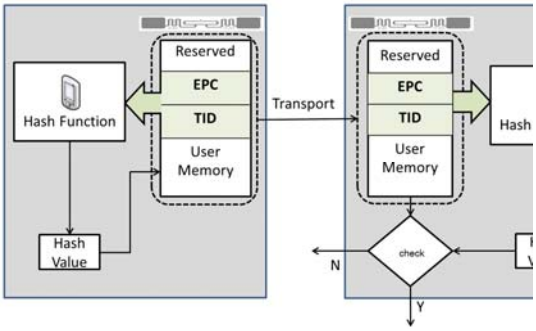

Figure 3. Encryption of tag data

A C-1 Gen-2 tag has four memory bank: reserved (bank 00), EPC (bank 01), TID (bank 10), and user (bank 11). Typically, the identifying code is stored in EPC bank and has the length of 96 bits. For serialized global trade item number (SGTIN), the first 14 bits are header, filter value, and partition. We choose the partition value to be 4 that divide the EPC code as in Table 1. Originally, SGTIN has three fields denoting company prefix, item reference, and serial number and they are recorded as integer values. The company is further divided into two parts: the first part is a four-digit (000-999, 10 bits) country code and the second part is a five-digit (00000-99999, 17 bits) authority code. The item

reference is divided into two fields: the first part is a three-digit (000-999, 10 bits) year and a two-digit (00-99, 7 bits) case word. The serial number occupies 12 bits which can be up to the 12-digit integer 274,877,906,943. The authority code and the case word are padded with 0's, if they are short than 5 and 2 digits, respectively. For example, sgtin:4.88607014.10207.54321 denotes partition value 4, country code 886, authority code 7014, year 102, case word 7, and serial number 54321.

The personnel and evidence items are attached a C-1 Gen-2 tag, either in the form of a badge or a sticker. Several evidence of one case may be place together in an evidence bag. An evidence bag will be sealed with a tag as well. The sealing tag is used once only, it will be destroyed when the bag is unsealed. When the evidence bag is resealed, a new tag is replaced to guarantee no unauthorized person can open the bag.

C. Tag Security Mechanism

It is important to protect no tags used in the chain of evidence custody cannot be cloned and tag data cannot be modified by unauthorized persons [7]. First, the access password and kill password are set to non-zero values by the

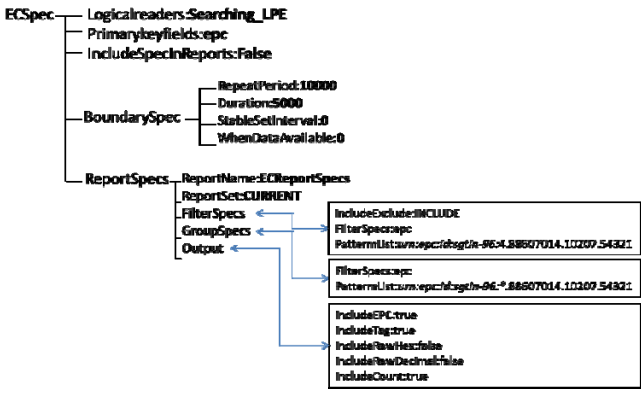

Figure 4. ALE ECSpec

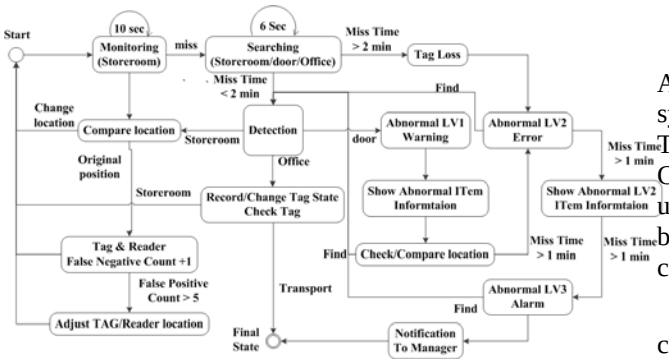

Figure 5. Evidence Storeroom Monitoring State Diagram.

system so the tag data can only be read, but not written. A hash mapping is performed by the reader to encode the EPC and TID bit stream and stored the hash value in the user bank as shown in Figure 3. The reader can also read EPC, TID, and data from the user bank to verify if the data is cloned tag. This method is different from most RFID security mechanisms because we consider it is possible to modify the firmware of a reader, but it is hardly to change tag functions.

D. Evidence Storeroom Monitoring

We describe how tag data are collected by ALE in an evidence storeroom. First, all readers in the chain of evidence custody are connected to ALE by the internet. A reader's behavior is specified by an ECSpec as shown in Figure 4. The ECSpec states that the reader is named as searching_LPE and will read EPC code primarily. The reader will be activated every 10 seconds (10000 μsec) and in each cycle it will continuously read 5 seconds (5000 μsec). The ECSpec is designed to search a lost physical evidence and to filter the data of sgtin:4.88607014.10207.54321.

In Figure 5. we show the state diagram of an evidence storeroom monitoring for searching lost physical evidence. Once the system detect the tag of an evidence item in the storeroom cannot be read, it assumes the evidence is missing. When the missing evidence is not read by a reader for 12 cycles, i.e., near two minutes, the alarm module will be activated to send first abnormal warning message. The system tries to read missing evidence continuously until it is found or the second error to report and abnormal error message. At the time when the third abnormal message is sent to evidence manager, it has a very high chance the evidence is missing for some reason.

The monitoring system will record all events observed including persons who get in touch with the evidence and entering the storeroom. When a missing evidence occurs, the recorded events can be traced to find out the reason and/or flaws of the missing evidence.

IV. SCENARIO SIMULATION

The monitoring system is implemented using ALE middleware and EPCIS event repository systems developed by Intelligent Identification Technology and Research Center (IITRC) at Feng Chia University. Readers and tags are simulated using a SimReader/SimTag system, also developed by IITRC. These systems constitute the major components of EPCglobal Architecture Framework.

We present collection of three scenarios: collecting crime scene data, packing and packing evidence bag, and monitoring of evidence storeroom as below.

A. Collecting Crime Scene Data

All the physical evidences at the scene are the originals and they are also the beginning of the chain of custody evidence. Hence, it is necessary to

read all the evidence type, quantity and identity of the people involved. Each of evidences and the law enforcement officer data is recorded as an object event and stored in the EPCIS event repository.

Figure 6. shows an example of crime scene evidence data. It includes the data of the officer in charge of collecting the evidence and all evidence items. The officer and evidence identifications are encoded with the coding format in Table 1. After evidences are collected from a crime scene, any person, such as forensics, prosecutor, storeroom keeper, who has contact with the evidence, will also, be recorded as an EPCIS event. Figure 7. shows an example of the evidence list. In addition, the events in the evidence list require signature confirmation to enhance the legal procedure.

B. Packing and Uacking Evidence Bag

Several evidence items of a crime may be collected and packed in an evidence bag which is sealed by affixing a one-time use tag. Sometimes, the sealed bag may need to be unpacked. For example, a closed crime case may be reopened because a secret witness appears after a number of years. In this case, the sealed evidence bag will be unpacked and re-examined.

To conduct unpacking of the sealed bag, the tag on the bag will be killed and is recorded as a deletion event. When the bag is repacked, a new tag is affix on the bag and is recorded an active event. Events of unpacking and repacking sealed bags are illustrated in Figure 8.

C. Monitoring of Evidence Storeroom

Sometimes, an abnormal condition of evidence m a y

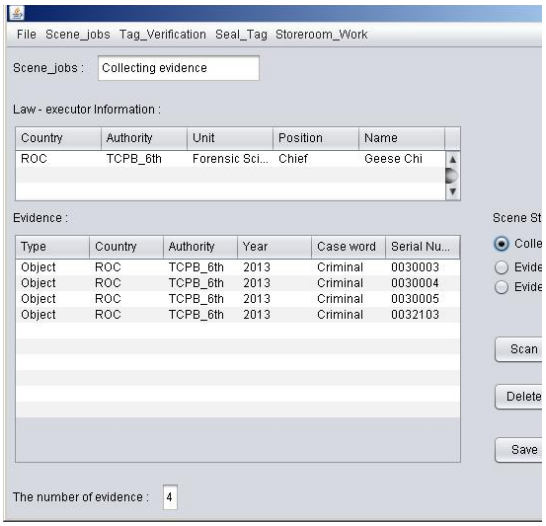

Figure 6. Crime scene evidence data

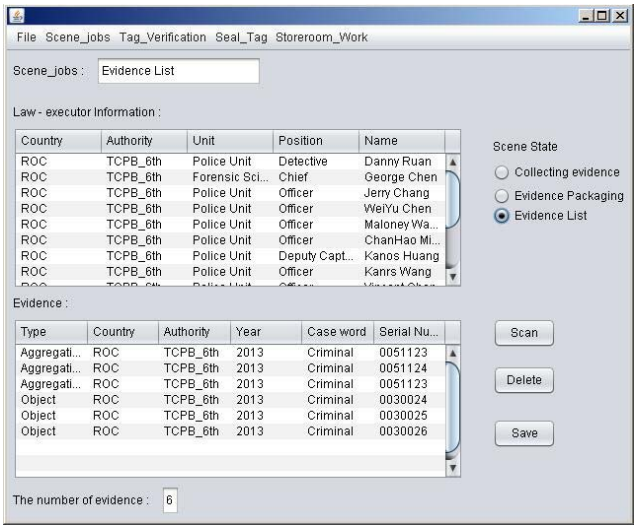

Figure 7. Evidence List

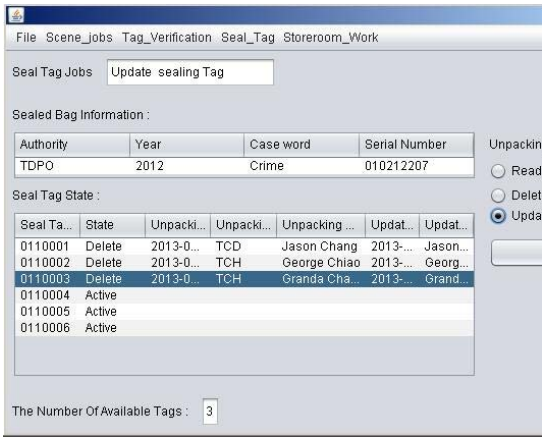

Figure 8. Unpacking and repacking sealed bag.

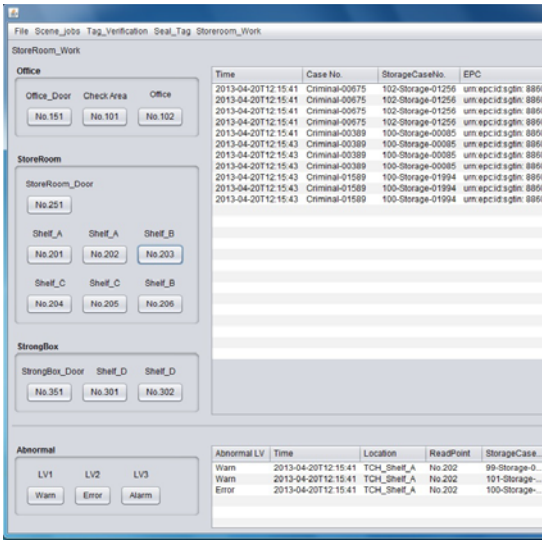

Figure 9. Evidence Storeroom Monitoring

occurs. Figure 9. shows an illustration of evidence storeroom monitoring record. It indicates office, storeroom, and shelf locations as the readpoints. The

EPC of evidence items and evidence bags are listed in the monitoring screen. In addition, abnormal message is shown in real-time when missing evidence is detected.

The storeroom door, the office door, and the check area are also installed with readers and infrared sensors. When some goes through these areas with tagged evidences, an infrared sensor will trigger the corresponding reader to read the EPC codes of the person and evidences and the event is recorded as a temporarily_transfer action. The system can verify the authorization of this action in real-time.

V. CONCLUSION

Current evidence custody uses signature procedure to construct a chain of custody of evidence. This by-human-chain approach has been proven that it is unable to meet the operation requirement. For example, evidence is not able to be monitored around the clock and evidence exception may occur that the custody officer is unable to effectively deal with the situation immediately.

We present the application of EPCglobal Architecture Framework to enhance the chain of evidence custody. This work is an extension of RFID technology and EPCglobal Architecture Framework from global supply chain management to legal administration management. The monitoring system is not only suitable for chain of evidence custody, but it can also be used in protection of precious goods. The system is characterized with the following advantages:

1) Evidence correctness:

RFID tags security verification, detection of damaged and misplaced evidence bags, and evidence identification on the transfer list and items ensure integration for the chain of evidence custody Evidence presented in the court is the same as that when it is collected.

2) Evidence Control Automation:

With RFID technology and EPCglobal Architecture Framework the evidence control is automated. Since all events taking place with the evidence and relevant personnel are all recorded, the data volume generated in the chain of evidence custody is very huge. Without an automatic system, data collection and processing is a tedious job and it is difficult to be done by human beings.

3) Real-time monitoring:

With the automated monitoring system, abnormal situations can be detected right at the time they happen and also be handled in real-time. The event based system can be designed to record all relevant and interested events and checked by a complex event processing engine.

The monitoring system can prevent most of flaws in the chain of evidence custody. However, it still has weakness when encountering malicious damage r embezzlement. One of the solutions is to combine surveillance video camera to monitor the evidence scene around the clock. With RFID technology and surveillance video camera, the video tape can be examined to catch the spoiler once a flaw happens.

REFERENCES

[1] J. Cosic and M. Baca , “Proving Chain of Custody and Digital Evidence Integrity,” MIPRO, Proceedings of the 33rd International Convention, pp. 1226-1230, 2010.

[2] M. Darianian, M. P. Michael, “Smart Home Mobile RFID-Based Internet-of-Things Systems and Services”, *Proceedings of International Conference on Advanced Computer Theory and Engineering*, 2008, pp. 116-120.

[3] EPCglobal. The Application Level Events (ALE) Specification, Version 1.1.1 Part I: Core Specification. Ratified standard, GS1, EPCglobal, 2009.

[4] EPCglobal. Core Business Vocabulary Standard. Ratified standard, GS1, EPCglobal, 2010.

[5] EPCglobal. “EPC Information Services (EPCIS) Version 1.0.1 Specification,” Technical report, GS1, EPCglobal, 2007.

[6] EPCglobal. EPCglobal Tag Data Standards Version 1.6. Ratified standard, GS1, EPCglobal, 2011.

[7] B. Fabian, T. Ermakova and C. Müller, "SHARDIS: A Privacy-Enhanced Discovery Service for RFID-Based Product Information," *IEEE Transactions on Industrial Informatics*, Vol. 8, No. 3, 2012, pp. 707-718.

[8] D. Gyllstrom, E. Wu, H. Chae, Y. Diao, P. Stahlberg, and G. Anderson. “SASE: Complex Event Processing over Streams,” *Proceedings of the Third Biennial Conference on Innovative Data Systems Research*,2007, pp. 407–411.

[9] X. Jin, X. Lee, N. Kong and B. Yan, “Efficient Complex Event Processing over RFID Data Stream,” *Proceedings of the Seventh IEEE/ACIS International Conference on Computer and Information Science*, 2008, pp. 75-81.

[10] D. Luckham, *The Power of Events: An Introduction to Complex Event Processing in Distributed Enterprise Systems*, Addison Wesley, 2002.

[11] M. G. Nagaraya,“Investigators Chain Of Custody In Digital Evidence Recovery,” Bureau of Police Research and Development, *Indian Police Journal*, 2006.

[12] National Police Agency, Ministry of the Interior, Republic of China, “Forensic Specification,” 2006.

[13] National Police Agency, Ministry of the Interior, Republic of China,“Police Crime Detection Manual,” 2008.

[14] K. Traub, F. Armenio, H. Barthel, P. Dietrich, J. Duker, C. Floerkemeier, J. Garrett, M. Harrison, B. Hogan, J. Mitsugi, J. Preishuber-Pfluegl, O. Ryaboy, S. Sarma, K. Suen, and J. Williams. The EPCglobal Architecture Framework, Final Version 1.4. Technical report, GS1, EPCglobal, 2010.

[15] F. Wang, S. Liu, and P. Liu. Complex RFID Event Processing. The VLDB Journal, Vol. 18, No. 4, 2009, pp. 913–931.

[16] P. Zhou, B. Cheng, J. Chen, “A Complex Event Processing based Alarm System for Coal Mine Safety Monitoring,” International Conference on Computer Science and Network Technology pp. 943-947, 2011.