TTA Standard

정보통신단체표준(영문표준)

TTAE.OT-xx.xxxx-Part1 제정일: 2018년 xx월 xx일

전자상거래 비즈니스 데이터의 생명주기 관리를 위한 보안 참조 구조

Security reference architecture for lifecycle management of e-commerce business data

TTA 한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회 응용보안 및 평가인증 프로젝트그룹(PG504)

표준안 심의 위원회 정보보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	염흥열	순천향대학교/개인 정보보호표준포럼	교수/의장	위원	
표준 초안 작성자	염흥열	순천향대학교/개인 정보보호표준포럼	교수/의장	위원	
	김지혜	순천향대학교	연구원	-	
	김미연	순천향대학교	연구원	-	
사무국 담당	김재웅	TTA	단장	-	
	문서연	TTA	전임연구원		

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2018.xx

서 문

1 표준의 목적

본 표준은 전자 상거래 비즈니스 데이터의 생명 주기관리를 위한 보안 참조 아키텍처를 정의한다. 참조 아키텍처는 데이터 보안이 중요하고 네트워크의 기본 기술과 독립적인 다양한 종류의 전자 상거래 서비스 에코 시스템에 적용될 수 있다. 본 표준은 전자 상거래 서비스 생태계에서 종단간 보안을 제공하기 위해 필요한 데이터 보안 관련 아키텍처 요소를 정의한다. 이 표준의 목적은 전자 상거래 비즈니스 데이터의 수명주기 관리를 위한 보안을 달성하기 위한 세부 권장 사항을 개발하기 위한 토대가 되는 것이다.

2 주요 내용 요약

전자 상거래 서비스는 개방형 네트워크에서 온라인 쇼핑 및 기타 서비스를 제공하며 다음과 같은 몇 가지 특징과 이점을 제공합한다. 효율적이고 편리하며 광범위하다. 그러나 이러한 전자 상거래 서비스 생태계는 보안 취약성에 직면해 있다. 본 표준은 전자 상거래 시스템이 직면 한 보안 위협을 분석하고 전자 상거래 비즈니스 데이터의 생명주기 관리를 위한 보안 참조 아키텍처를 제공한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

이 표준은 다음 인용표준을 영문 그대로 완전 수용하는 표준이다.

Recommendation ITU-T X.1040(2017), Security reference architecture for lifecycle management of e-commerce business data

3.2 인용 표준과 본 표준의 비교표

TTAE.xx-xx.xxxx	ITU-T X.1040	비고
1. 범위	1. Scope	동일
2. 정규 참고문헌	2. References	동일
3. 정의	3. Definitions	동일
4. 약어	4. Abbreviations and acronyms	동일
5. 범주	5. Conventions	동일
6. 전자상거래 서비스 특징	6. Characteristics of e-commerce service	동일
7. 보안 위협	7. Security threats	동일
8. 보안 대책	8. Security dimensions	동일
9. 보안 참조 구조	9. Security reference architecture	동일
참고문헌	Bibliography	동일

Preface

1 Purpose

This Recommendation defines a security reference architecture for the lifecycle management of e-commerce business data. The reference architecture can be applied to various kinds of e-commerce service ecosystems where data security is of concern and independent of the network's underlying technology. This Recommendation defines data security-related architectural elements that are necessary for providing end-to-end security in e-commerce service ecosystems. The objective of this Recommendation is to serve as a foundation for developing the detailed recommendations to achieve security for the lifecycle management of e-commerce business data.

2 Summary

E-commerce services provide online shopping and other services in open networks, and have several characteristics and benefits: they are efficient, convenient and wide-reaching. However, these e-commerce service ecosystems face security vulnerabilities. Recommendation ITU-T X.1040 analyses the security threats faced by e-commerce systems, and provides a security reference architecture for lifecycle management of e-commerce business data.

3 Relationship to Reference Standards

3.1 The relationship of international standards

The standard is fully equivalent to ITU-T X.1040, Security reference architecture for lifecycle management of e-commerce business data.

3.2 Differences between International standards(recommendation) and this standard

TTAE.xx-xx.xxxx	X.1040	Remarks
1. Scope	1. Scope	Equals
2. References	2. References	Equals
3. Definitions	3. Definitions	Equals
4. Abbreviations and acronyms	4. Abbreviations and acronyms	Equals
5. Conventions	5. Conventions	Equals
6. Characteristics of e-commerce service	6. Characteristics of e-commerce service	Equals
7. Security threats	7. Security threats	Equals
8. Security dimensions	8. Security dimensions	Equals
9. Security reference architecture	9. Security reference architecture	Equals
Bibliography	Bibliography	Equals

목 차

Recommendation ITU-TX.1040

Security reference architecture for lifecycle management of e-commerce business data

1 Scope

This Recommendation defines a security reference architecture for the lifecycle management of e-commerce business data. The reference architecture can be applied to various kinds of e-commerce service ecosystems where data security is of concern and independent of the network's underlying technology. This Recommendation defines data security-related architectural elements that are necessary for providing end-to-end security in e-commerce service ecosystems. The objective of this Recommendation is to serve as a foundation for developing the detailed recommendations to achieve security for the lifecycle management of e-commerce business data.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications.*

3 Definitions

3.1Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 **accountability** [b-ITU-T X.800]: The property that ensures that the actions of an entity may be traced uniquely to that entity.

3.1.2 **authentication** [b-ITU-T X.1601]: Verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

3.1.3 **authorization** [b-ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

3.1.4 **availability** [b-ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.5 **confidentiality** [b-ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.6 **data** [b-ITU-T G.9960]: Bits or bytes transported over the medium or via a reference point that individually convey information. Data includes both user (application) data and any other auxiliary information (overhead, including control, management, etc.). Data does not include bits or bytes that, by themselves, do not convey any information, such as the preamble.

3.1.7 **data integrity** [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.8 **data security** [b-ISO/IEC 29182-2]: Preservation of data to guarantee availability, confidentiality and data integrity.

3.1.9 **information** [b-ITU-T X.902]: Any kind of knowledge, that is exchangeable amongst users, about things, facts, concepts and so on, in a universe of discourse. Although information will necessarily have a representation form to make it communicable, it is the interpretation of this representation (the meaning) that is relevant in the first place.

3.1.10 **threat** [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.

3.1.11 **sensitive data** [b-ISO 5127]: Data with potentially harmful effects in the event of disclosure or misuse.

3.2Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 **data lifecycle management**: Defines how data are managed and maintained as it flows through the business processes across all phases of the data lifecycle.

3.2.2 **data transmission**: The process of transferring data from one place to another place by communication.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

B2B	Business to Business
B2C	Business to Customer
C2C	Customer to Customer
CRM	Customer Relationship Management
DDoS	Distributed Denial of Service
DoS	Denial of Service
ISV	Independent Software Vendor

5 Conventions

None.

6 Characteristics of e-commerce service

Clauses 6.1 and 6.2 describe the characteristics of e-commerce service.

6.1 Parties and business processes of e-commerce service

An e-commerce service ecosystem mainly includes these parties: seller, buyer, e-commerce platform, independent software vendor (ISV), payment platform and logistics platform.

The main processes between the seller and the e-commerce platform include: user registration, product display, order handling, payment handling and product shipping.

The main processes between the buyer and the e-commerce platform include: user registration, product browsing, product ordering, product payment and product shipping.

The main process between the ISV and the e-commerce platform is order handling.

The main process between the e-commerce platform and the payment platform is payment handling.

The main process between the e-commerce platform and the logistics platform is shipping handling.

The interworking model among these parties is shown in Figure 1:

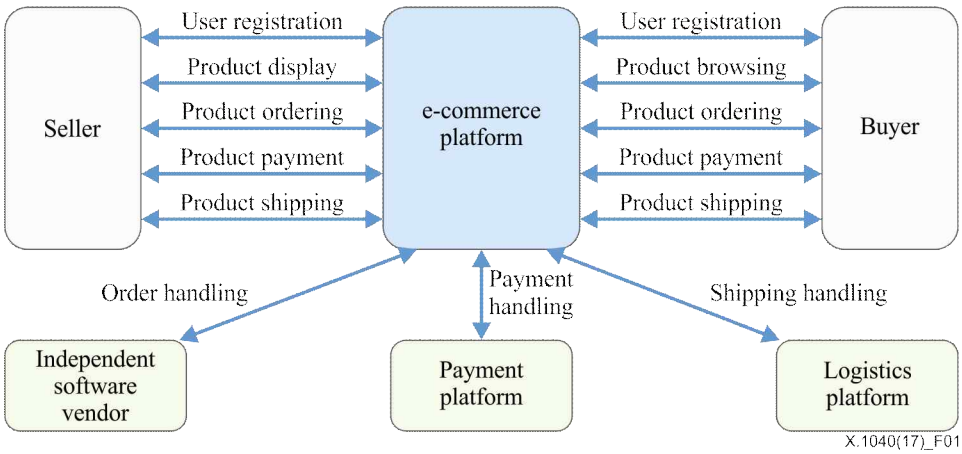

Figure 1 – E-commerce service interworking model

The seller is a party that sells products in the e-commerce platform; the seller can be an enterprise or an individual.

The buyer is a party that buys products in the e-commerce platform; the buyer can be an enterprise or an individual.

The e-commerce platform is the core part of the model and is responsible for trade between the seller and the buyer, and includes the functions of user registration, product display, product ordering, product payment and product shipping. It also interacts with: the ISV for order handling, the payment platform for payment handling, and the logistics platform for shipping handling.

The ISV is a party that produces independent software to be used in the e-commerce platform, and this software can provide order handling services to buyers and sellers, and also other services, e.g., customer relationship management (CRM) service, inventory management service.

The payment platform is a party that provides payment services to the e-commerce platform, and it helps the buyers and sellers to perform payment transactions.

The logistics platform is a party that provides logistics services to the e-commerce platform, and it helps the buyers and sellers to ship the products.

The e-commerce service interworking model is a high-level logical conceptual diagram for

typical e-commerce services. E-commerce services have various business models. In some business models, sellers can be integrated into the e-commerce platform. Also, the ISV, payment platform and logistics platform can be integrated into the e-commerce platform, depending on their different business models.
The e-commerce service ecosystem may employ the following forms:

- business to business (B2B): The e-commerce business data are exchanged between enterprises;
- business to customer (B2C): The e-commerce business data are exchanged between an enterprise and an individual customer;
- customer to customer (C2C): The e-commerce business data are exchanged between an individual seller and an individual buyer.

6.2 Data in the e-commerce service

In the e-commerce service ecosystem, e-commerce business data need to be managed and maintained as it flows through the business processes across all phases of the data lifecycle. The data lifecycle management can include various phases, including data creation, data usage, data storage, data transmission and data destruction.
The lifecycle management of e-commerce business data have the following security challenges:

- the security border of the organizations becomes blurred and disappears;
- frequent data exchange and data sharing bring more opportunities for data leakage;
- sensitive data can be derived from data linkage, data combination and data analysis;
- security issues may occur during the entire data lifecycle management, from creation to destruction;
- data exchange and sharing among organizations is frequent, and security becomes a common issue for the entire e-commerce service ecosystem.

It is necessary to define a common security reference architecture for lifecycle management of e-commerce business data, to provide guidance to all the parties in the e-commerce service ecosystem to understand and overcome these challenges.
In the e-commerce service ecosystem, there is a great deal of data. In this Recommendation, data refers to e-commerce business data, excluding financial transaction data. The e-commerce business data refer to e-commerce business-related data in the e-commerce service ecosystem, which includes registration-related data, order-related data, product-related data, and shipping-related data.
Examples of e-commerce business data are:

- order related data: Order identifier, creation time, product identifier, product amount.
- product related data: Product identifier, product name, product description, product category, product parameters (e.g., brand, type, colour, size), product amount.

7 Security threats

The security architecture defines a plan and set of principles that describes a security structure for the data lifecycle management security solution. The architecture identifies security issues that need to be addressed to prevent both intentional, as well as accidental threats.

The following threats are identified during the lifecycle management of e-commerce business data:

- data disclosure:
  - data are viewed, accessed or stolen by unauthorized users;
  - data are intentionally or unintentionally published or resold by authorized users.
- data modification:
  - data are changed by unauthorized users, computer viruses, faulty disks, power failures, etc.;
  - authorized users intentionally or unintentionally modify data.
- data destruction:
  - data are accidentally/maliciously removed or destroyed during a system crash, by unauthorized users, or in unexpected situations.
- data unavailable:
  - data are temporarily or permanently unavailable due to events such as data loss, data being encrypted by malicious attackers.
- data misuse:
  - data are deviated from their intended use by authorized users, that is, data are used for other purposes instead of their original purpose, either intentionally or unintentionally.
- data pollution:
  - data are contaminated with irrelevant, redundant, unsolicited, useless, undesirable, false or fake information.

8 Security dimensions

Table 1 describes the application of security dimensions for security objectives.

Table 1 – Applying security dimensions for security objectives

Security dimension	Security objectives
Confidentiality	Protect e-commerce business data that are transiting within the e-commerce service ecosystem or are resident in offline storages against unauthorized access or viewing.
Integrity	Protect e-commerce business data that are transiting within the e-commerce service ecosystem or are resident in offline storages against unauthorized modification, deletion, creation and replication.
Availability	Ensure that access to e-commerce business data resident in offline storages cannot be denied to authorized personnel (including end-users) and entities. This includes protection against active attacks such as denial of service (DoS) attacks as well as protection against passive attacks, such as the modification or deletion of authentication information (e.g., user identifications and passwords, administrator identifications and passwords).
Authentication	Verify the account of personnel or entities attempting to provide or access e-commerce business data, which are transiting within the e-commerce service ecosystem or are resident in offline storages.
Authorization	Ensure that only authorized personnel or entities are allowed to perform actions on the e-commerce business data.
Accountability	Provide a record identifying each person or entity that accessed e-commerce business data, which are transiting within the e-commerce service ecosystem or are resident in offline storages, and the action that was performed. This record is used as proof and allows tracing of access to the e-commerce business data.

Additional explanations for the security dimensions discussed above (including authentication, integrity, confidentiality, availability) can be found in [ITU-T X.805].

Table 2 provides a mapping of security dimensions to security threats.

Table 2 Mapping of security dimentions to security threat

Security threats / Security dimension	Data disclosure	Data modification	Data destruction	Data unavailable	Data misuse	Data pollution
Confidentiality	Y	Y				
Integrity		Y		Y		Y
Availability			Y	Y		Y
Authentication	Y	Y	Y		Y	Y
Authorization	Y	Y	Y		Y	Y
Accountability	Y	Y	Y	Y	Y	Y
NOTE – The letter 'Y' in a cell formed by the intersection of a column (security threat) and a row (security dimension) indicates that this particular security threat is the subject of the control provided by the corresponding security dimension.						

9 Security reference architecture

9.1 Architectural diagram

The reference architecture diagram for lifecycle management of e-commerce business data are shown in Figure 2:

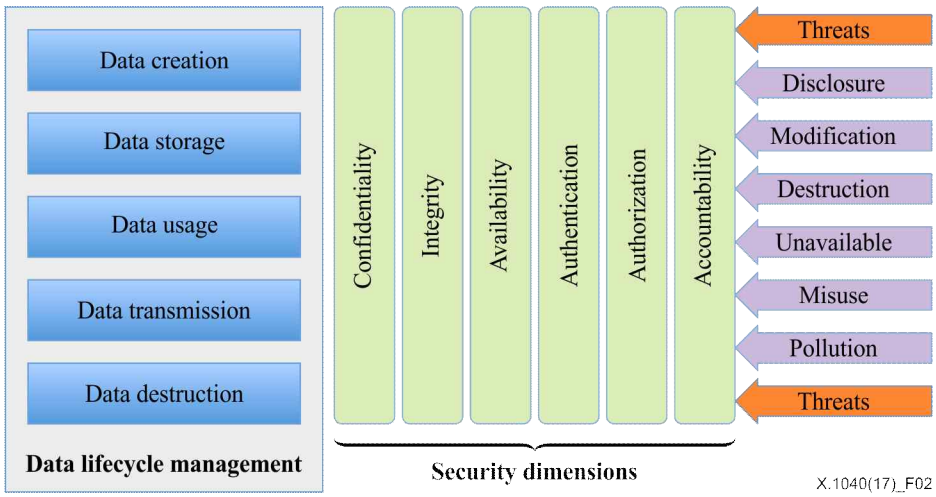

Figure 2 – Security reference architecture diagram

9.2 Data lifecycle management

9.2.1 Overview

The data lifecycle management mainly consists of five phases: data creation, data usage, data storage, data transmission and data destruction.
The data lifecycle management is described in Figure 3:

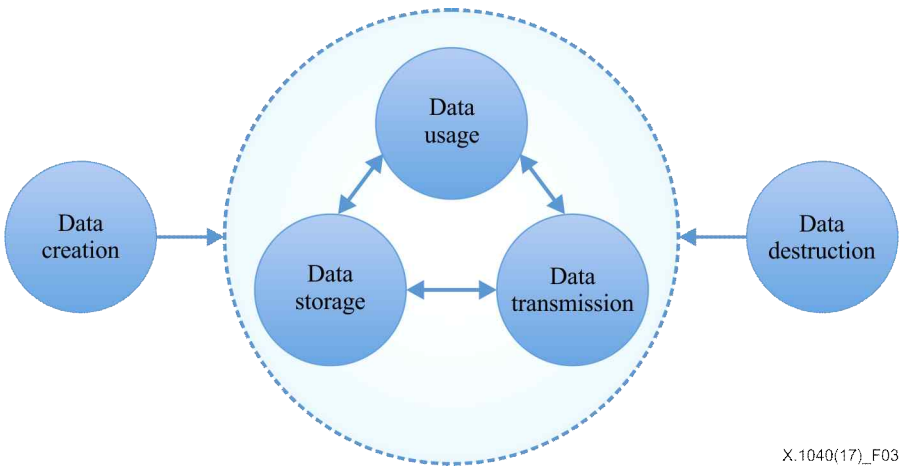

Figure 3 – Data lifecycle management

In data lifecycle management, data creation is the starting phase and data

destruction is the ending phase. After creation, data can be stored, transmitted or used. Data can be transferred between different phases, for example, after usage, data can be stored or transmitted; after storing, data can be used or transmitted; after transmission, data can be stored or used. After destruction, data may be recovered and regarded as created again. Not all the data need to go through all the phases; for example, data can be created, stored and destroyed, without transmission or usage.

9.2.2 Data creation

Data creation is the generation of new digital content, or the alteration/updating of existing content, either structured or unstructured.
This is the first phase of the e-commerce business data in the e-commerce ecosystem. In this phase, the main security objectives are:

- achieving and maintaining appropriate data protection by making sure that the data source is legally compliant, authenticated and that it actually owns the data;
- ensuring that the data gets an appropriate level of protection by being classified according to its value, legal requirements, sensitivity and essentiality.

9.2.3 Data storage

Data storage refers to inactive data, which is stored physically in any digital form. Storing is the act of committing the digital data to some sort of storage repository. Data storing typically occurs almost simultaneously with creation.
In this phase, the main security objectives are:

- preventing unauthorized disclosure, modification, removal or destruction of e-commerce business data stored on physical or cloud storage;
- ensuring that the e-commerce business data are securely stored according to their value, legal requirements, sensitivity and essentiality;
- ensuring that the e-commerce business data are protected at all times under business context and availability requirements.

9.2.4 Data usage

Data usage refers to the combination of a series of activities (e.g., viewed, analysed, processed) towards data.
In this phase, the main security objectives are:

- managing identities of entities that may be granted access to the e-commerce business data;
- restricting data access within appropriate least privilege based on business and security requirements;
- ensuring proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of the data;
- ensuring data security from unauthorized actions by capturing data access and usage activity with preventative or detective methods to stop security violations.

9.2.5 Data transmission

Data transmission is the process of transferring data between storage types, formats or computer systems.
In this phase, the main security objective is to ensure the protection of data transmitted within the e-commerce ecosystem, especially to ensure data integrity and confidentiality.

9.2.6 Data destruction

Data destruction refers to the process of permanently or temporarily making the data unavailable using physical or digital means (e.g., crypto-shredding, freezing data under business context).
In the case of temporary destruction, a backup operation should be made of the e-commerce business data, so that the e-commerce business data can be restored in the recovery case.
In this phase, the main security objectives are:

- ensuring that the data are effectively destroyed under legal, contractual compliance and security requirements;
- preventing unauthorized physical or cloud storage access, damage and interference to the e-commerce business data.

9.3Security dimensions for data lifecycle management

9.3.1 Confidentiality dimension

The confidentiality dimension protects e-commerce business data from unauthorized disclosure. Data confidentiality ensures that unauthorized personnel or entities cannot understand the data content. Encryption, access control lists and permissions are methods often used to provide data confidentiality.
The confidentiality dimension mainly applies to the data storage and data transmission phases.
In the data storage phase, e-commerce business data need to be encrypted and kept as confidential to avoid unauthorized access or disclosure from physical storage or cloud storage by unauthorized personnel or entities.
In the data transmission phase, e-commerce business data need to be encrypted and kept as confidential to prevent unauthorized diversion or interception during the transmission between two entities.

9.3.2 Integrity dimension

The integrity dimension ensures the correctness or accuracy of the data. The data are protected against unauthorized modification, deletion, creation, and replication and provide an indication of these unauthorized activities. Digital signature and digest verification are methods often used to provide data integrity and to avoid data non-repudiation.
The integrity dimension mainly applies to the data creation, data storage and data transmission phases.
In the data creation phase, integrity should be guaranteed to avoid improper data modification or destruction during the e-commerce business data creation process.
In the data storage phase, integrity should be guaranteed to avoid improper data modification or destruction to the e-commerce business data residing in physical or cloud storage.
In the data transmission phase, integrity should be guaranteed to avoid improper data modification or destruction to the e-commerce business data during the transmission between two entities.

9.3.3 Availability dimension

The availability dimension ensures that there is no denial of authorized access to stored data and data flows due to events impacting the data. One typical attack, which compromises data availability is a distributed denial of service (DDoS) attack, which is an attempt to make e-commerce business data unavailable by overwhelming the requested entity or service with massive amounts of traffic from multiple sources. DDoS protection is one of the mechanisms to provide data availability.
The availability dimension mainly applies to the data usage and data storage phases.
In the data usage phase, availability ensures that e-commerce business data are available for

use (e.g., access, view, analysis, process) by authorized personnel or entities. One important aspect is to protect the system/platform environment of the data usage to guarantee data availability.
In the data storage phase, availability ensures that e-commerce business data are available for physical or cloud storage by authorized personnel or entities. One important aspect is to securely configure physical or cloud storage to guarantee the consistent availability of the data storage environment.

9.3.4 Authentication dimension

The authentication dimension serves to confirm the identities of communicating personnel or entities. Authentication ensures the validity of the claimed identities of the entities participating in data communication (e.g., person, device, service, application) and provides assurance that an entity is not attempting a masquerade or unauthorized replay of a previous data communication. Authentication is also used to verify the claimed identities of the data source to ensure data authenticity. Credentials, certificates, biometrics, two-factor authentication are methods often used to provide authentication.
The authentication dimension applies to all data lifecycle management phases, including data creation, data usage, data storage, data transmission and data destruction.
In the data creation phase, authentication serves to confirm the identities of the personnel or entities that request to create and collect e-commerce business data, and to also confirm the identities of the data source.
In the data usage phase, authentication serves to confirm the identities of the personnel or entities that request to use (e.g., access, view, analysis, process) e-commerce business data.
In the data storage phase, authentication serves to confirm the identities of the personnel or entities that request to store e-commerce business data to physical or cloud storage.
In the data transmission phase, authentication serves to confirm the identities of the personnel or entities that request to send or receive e-commerce business data.
In the data destruction phase, authentication serves to confirm the identities of the personnel or entities that request to destroy e-commerce business data.

9.3.5 Authorization dimension

The authorization dimension provides the means for preventing an individual or entity from performing unauthorized actions related to e-commerce business data. It ensures that only an authorized individual or entity can perform specific actions (e.g., read, create, modify, delete) related to e-commerce business data. Access control, access rights and account management are mechanisms often used to provide authorization functionality.
The authorization dimension applies to all data lifecycle management phases, including data creation, data usage, data storage, data transmission and data destruction.
In the data creation phase, authorization ensures that only an authorized individual or entity can create and collect e-commerce business data.
In the data usage phase, authorization ensures that only an authorized individual or entity can use (e.g., access, view, analysis, process) e-commerce business data.
In the data storage phase, authorization ensures that only an authorized individual or entity can store e-commerce business data to physical or cloud storage.
In the data transmission phase, authorization ensures that only an authorized individual or entity can send and receive e-commerce business data.
In the data destruction phase, authorization ensures that only an authorized individual or entity can destroy e-commerce business data.

9.3.6 Accountability dimension

The accountability dimension provides the means for preventing an individual or entity from denying having performed a particular action related to data by providing evidence and trace of various actions (e.g., proof of obligation, intent, or commitment; proof of data origin, proof of ownership, proof of resource use). It ensures the availability of evidence that can be

presented to a third party and used as proof that some kind of event or action had taken place. Logging and tracing are mechanisms often used to provide accountability.
The accountability dimension applies to all data lifecycle management phases, including data creation, data usage, data transmission, data storage and data destruction.
In the data creation phase, accountability provides the means for preventing an individual or entity from denying having performed data creation actions related to e-commerce business data by making available proof and trace of data creation actions.
In the data usage phase, accountability provides the means for preventing an individual or entity from denying having performed data usage actions (e.g., access, view, analysis, process) related to e-commerce business data by making available proof and trace of data usage actions (e.g., access, view, analysis, process).
In the data storage phase, accountability provides the means for preventing an individual or entity from denying having performed data storage actions related to e-commerce business data by making available proof of, and tracing of, data storage actions.
In the data transmission phase, accountability provides the means for preventing an individual or entity from denying having performed data transmission actions (e.g., send, receive) related to e-commerce business data by making available proof and trace of data destruction actions (e.g., send, receive).
In the data destruction phase, accountability provides the means for preventing an individual or entity from denying having performed data destruction actions related to e-commerce business data by making available proof and trace of data destruction actions.

9.4Applying security dimensions for data lifecycle management

Table 3 provides a mapping of security dimensions to the data lifecycle management of e-commerce business data.

Table 3 – Applying security dimensions to data lifecycle management

Data lifecycle / **Security dimension**	**Data creation**	**Data usage**	**Data transmission**	**Data storage**	**Data destruction**
Confidentiality			Y	Y	
Integrity	Y		Y	Y	
Availability		Y		Y	
Authentication	Y	Y	Y	Y	Y
Authorization	Y	Y	Y	Y	Y
Accountability	Y	Y	Y	Y	Y
NOTE – The letter 'Y' in a cell formed by the intersection of a column (data lifecycle) and a row (security dimension) designate that this security dimension applies to the corresponding data lifecycle management phase.					

1.

Bibliography

[b-ITU-T G.9960] Recommendation ITU-T G.9960 (2015), *Unified high-speed wireline-based home networking transceivers - System architecture and physical layer specification.*

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications.*

[b-ITU-T X.902] Recommendation ITU-T X.902 (2009) | ISO/IEC 10746-2:2010, *Information technology - Open Distributed Processing - Reference model: Foundations*.

[b-ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing.*

[b-ISO 5127] ISO 5127:2017, *Information and documentation - Foundation and vocabulary.*

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology - Security techniques - Information security management systems - Overview and vocabulary.*

[b-ISO/IEC 29182-2] ISO/IEC 29182-2:2013, *Information technology - Sensor networks: Sensor Network Reference Architecture (SNRA) Part 2: Vocabulary and terminology.*

부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

Ⅰ-1.1 지식재산권 확약서(1)

- 해당 사항 없음

Ⅰ-1.2 지식재산권 확약서(2)

- 해당 사항 없음

※ 상기 기재된 지식재산권 확약서 이외에도 본 표준이 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

Ⅰ-2.1 시험인증 대상 여부

- 해당 사항 없음

Ⅰ-2.2 시험표준 제정 현황

- 해당 사항 없음

부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

- 해당 사항 없음

부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

- 해당 사항 없음

부 록 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

Ⅰ-5.1 표준의 목적 및 용도

이 표준은 전자 상거래 비즈니스 데이터의 생명 주기관리를 위한 보안 참조 아키텍처를 정의한다. 참조 아키텍처는 데이터 보안이 중요하고 네트워크의 기본 기술과 독립적인 다양한 종류의 전자 상거래 서비스 에코 시스템에 적용될 수 있다. 이 표준은 전자 상거래 서비스 생태계에서 종단간 보안을 제공하기 위해 필요한 데이터 보안 관련 아키텍처 요소를 정의한다. 이 표준의 목적은 전자 상거래 비즈니스 데이터의 수명주기 관리를 위한 보안을 달성하기 위한 세부 권장 사항을 개발하기 위한 토대가 되는 것이다.

Ⅰ-5.2 전자상거래 주요 특징 (6장)

이 절에서는 전자상거래의 주요 특징을 제시한다. 전자 상거래 플랫폼과 물류 플랫폼 간의 주요 프로세스는 운송 처리이다. 이들 당사자 간의 인터 워킹 모델은 그림 1에 나와 있다.

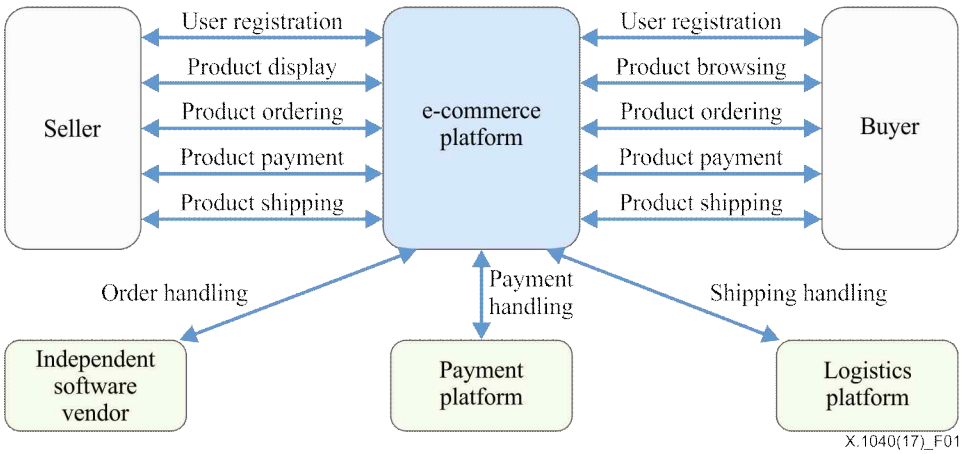

그림 Ⅰ-5-1 – 전자상거래 서비스 상호동작 모델

Ⅰ-5.3 보안 위협 (7장)

보안 아키텍처는 데이터 수명주기 관리 보안 솔루션의 보안 구조를 설명하는 계획 및 원칙 집합을 정의한다. 이 아키텍처는 고의적 위협뿐만 아니라 우발적 위협을 방지하기 위해 해결해야 할 보안 문제를 식별한다.

Ⅰ-5.4 보안 대책(8장)

이 절에서는 보안 목적을 위한 보안 차원의 적용을 기술한다.

Ⅰ-5.5 보안 참조 구조(9장)

전자 상거래 비즈니스 데이터의 라이프 사이클 관리에 대한 참조 아키텍처 다이어그램은 다음 그림과 같다.

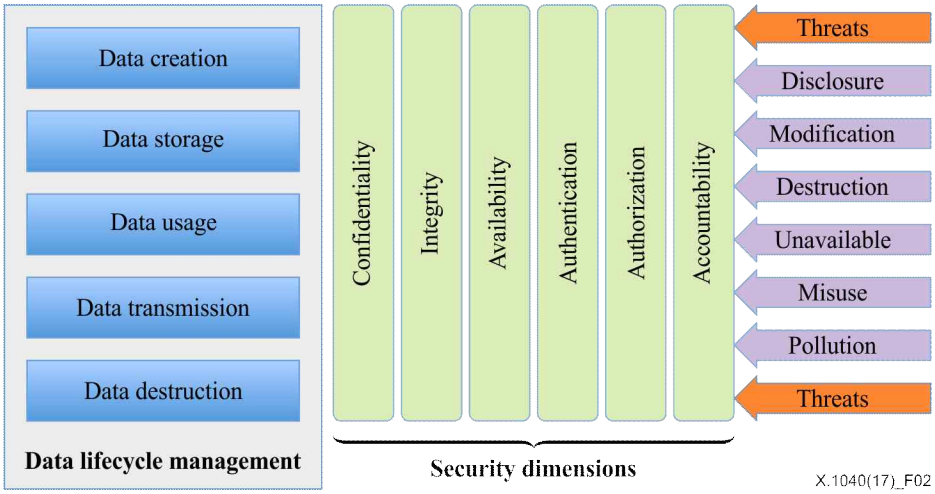

그림 Ⅰ-5-2 – 보안 참조 구조도

부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2018.XX.XX	제정 TTAE.OT-xx.xxxx	전자상거래 비즈니스 데이터의 쟁명주기 관리를 위한 보안 참조 구조	PG504