International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 35

(09/2019)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1254 – Supplement on use cases of the entity authentication assurance framework

ITU-T X-series Recommendations – Supplement 35

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	X.1700–X.1729

For further details, please refer to the list of ITU-T Recommendations.

Supplement 35 to ITU-T X-series Recommendations

ITU-T X.1254 – Supplement on use cases of the entity authentication assurance framework

Summary

Supplement 35 to ITU-T X-series Recommendations on Recommendation ITU-T X.1254 contains three use cases of applying the entity authentication assurance framework in security implementation, including detailed security considerations in risk assessment, choice of appropriate assurance level and selection of authentication technologies.

The use cases described in this Supplement can assist the deployment of enhanced authentication solutions in various environments, including telecommunication and Internet transactions.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X Suppl. 35	2019-09-05	17	11.1002/1000/14066

Keywords

Authentication assurance, use cases.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Supplement 35 to ITU-T X-series Recommendations

ITU-T X.1254 – Supplement on use cases of the entity authentication assurance framework

1 Scope

This Supplement to [ITU-T X.1254] contains three use cases of applying the entity authentication assurance (EAA) framework in security implementation, including detailed security considerations in risk assessment, choice of appropriate assurance level and selection of authentication technologies.

2 References

[ITU-T X.1254] Recommendation ITU-T X.1254 (2012), *Entity authentication assurance framework.*

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 authentication factor [b-ITU-T X.1154]: A type of credential; there are three types of authentication factors: ownership factor, knowledge factor and biometric factor.

NOTE – Authentication factors are divided into four categories:

– something an entity has (e.g., device signature, passport, hardware device containing a credential, private key);

– something an entity knows (e.g., password, personal identification number (PIN));

– something an entity is (e.g., biometric characteristic);

– something an entity typically does (e.g., behaviour pattern).

3.1.2 entity authentication assurance (EAA) [ITU-T X.1254]: A degree of confidence reached in the authentication process that the entity is what it is, or is expected to be.

3.2 Terms defined in this Supplement

This Supplement defines the following term:

3.2.1 telecommunication scam: Fraud that makes use of a telecommunication service provided by a telecommunication service operator.

NOTE – This definition is based on that for telephone service scam in [b-ITU-T X-Sup.33].

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

CSP Credential Service Provider

DLT Distributed Ledger Technology

EAA Entity Authentication Assurance

LoA Level of Assurance

MD5 Message Digest algorithm 5

MitM	Man-in-the-Middle
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RSA	Rivest, Shamir and Adleman
SDK	Software Development Kit
SIM	Subscriber Identity Module
SMS	Short Message Service
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module

5 Conventions

None.

6 Use case 1: Self-service SIM card replacement

The telecommunication scam has historically been one of those most commonly seen. Along with the fast growth of mobile Internet, smartphones have become indispensable for many people in their daily lives. More and more mobile apps, including mobile banking apps, are installed on smartphones. More and more personally identifiable information (PII) is stored on smartphones. Smartphone is becoming a more and more high-value target for scammers today and will continue to be so for the foreseeable future.

In this clause, a typical telecommunication scam targeting self-service subscriber identity module (SIM) card replacement is examined in detail. The business flow and its security flaws are examined. The detailed attack process is introduced. An analysis of how to avoid such a telecommunication scam is discussed.

6.1 Business workflow

Today, the smartphone is a fashion item for the young generation and is replaced every 2 or 3 years. Technology development is making SIM cards ever smaller to fit into more compact, yet more powerful smartphones. Hence, one common service provided by telecommunication operators is the replacement of a customer's original SIM card with a new and frequently smaller universal subscriber identity module (USIM) card, which usually retains the original phone number for the customer. If this service is provided in the telecommunication operator's business office, the operator's costs increase and the customer has to pay a time-consuming physical visit, but the service is generally secure.

Operators have also set up a new self-service for customers to perform this operation online to avoid the customer visit to the local business office. Initially, a straightforward business workflow is designed and described as follows.

1) A customer wants to replace his or her SIM card with a new USIM card. He or she goes to the operator's website and initiates the application process online.
2) He or she creates a user account by registering a username, password, postal address and phone number.
3) The USIM card requested is sent to the registered postal address.
4) After receiving the USIM card, the customer logs on to his or her user account using the registered username and password, and requests activation of the USIM card online.

5) A verification code is sent via short message service (SMS) to the registered phone number.

6) The customer inputs the verification code online.

7) The original SIM card is revoked. The USIM card is activated to replace it.

In this workflow, steps 5) and 6) are essential to verification. The precondition and presumption of secure operation is that the initiator of this self-service workflow is also the owner of the original SIM card and the only person who can receive and input the verification code online.

Unfortunately, this workflow is susceptible to hacking, as described in clause 6.2.

6.2 Hacking the business workflow

The self-service workflow outlined in clause 6.1 can be exploited by hackers for social-engineering attacks, as described in Table 6-1.

Table 6-1 – Process of social-engineering attacks

Hacker	Victim and owner of the SIM card
1. A victim is chosen because a hacker somehow gets hold of the victim's phone number. The hacker initiates the application process online	Have no idea what is happening.
2. The hacker goes to the operator's website and registers an account with the victim's phone number, but with the hacker's postal address	Have no idea what is happening.
3. The hacker applies for a new USIM card using the registered victim's account; the new card is sent to the hacker's postal address	Have no idea what is happening.
4. The hacker tries to hoax the victim to give him or her the necessary information. The hacker sends an SMS to the victim, saying something like: "We have subscribed you to service X…, to unsubscribe, please reply with the verification code"	
	5. The victim receives the SMS message, has no clue of what is going on, and starts wondering about how to unsubscribe
6. The hacker requests replacement of the original SIM with the new USIM card online. The system automatically sends an SMS with the verification code to the phone with the original SIM card	
	7. The victim receives an SMS message like the one below with a verification code and is hoaxed into believing that he or she has subscribed to service X, and want to unsubscribe. "…the verification code is YYY"
	8. The victim replies to the hacker's SMS with the verification code YYY in order to unsubscribe

Table 6-1 – Process of social-engineering attacks

Hacker	Victim and owner of the SIM card
9. The hacker receives the verification code YYY, which he or she needs to revoke the original SIM card and activate its replacement USIM. The hacker inputs the code online, and the new USIM card begins to work inside the hacker's phone.	
	10. The victim's phone is out of service and he or she has lost control of the SIM card
11. The hacker can then use the USIM card to hack the victim's mobile banking account, online shopping account, etc., e.g., by resetting passwords of these accounts by SMS	

6.3 Risk assessment

Before designing the business workflow of this self-service as described in clause 6.1, risk assessment, including risk identification, risk analysis and risk evaluation, should be conducted. In this way, proper security control methods can be correspondingly chosen to mitigate identified risks.

In this use case, the smartphone user's original SIM card is revoked, while a new USIM card is activated. If erroneous authentication happens in this process, or if hacker attacks succeed in ways similar to those described in clause 6.2, there will be substantial risk for the smartphone user as the original user will not only lose control of the phone number, but may also suffer financial loss due to abuse of phone number-associated mobile payment accounts. The user may also face privacy information leakage, as some social networking accounts may be associated with the phone number. Furthermore, operators may be blamed for not being able to provide enough protection for their provisioned services and suffer reputation and loyalty loss from customers.

Hence, based on [ITU-T X.1254], this self-service requires a level of assurance 3 (LoA3) authentication through which high confidence in the claimed or asserted identity of the smartphone user is acquired. Multifactor authentication should be employed, and any secret information exchanged in authentication protocols shall be cryptographically protected in transit and at rest (although LoA3 does not require the use of a cryptographically based challenge-response protocol).

6.4 Risk mitigation approaches

In this use case, risk assessment identifies threats include, but are not limited to, lost or stolen smartphone, social engineering attack, impersonation attack, man-in-the-middle (MitM) attack, PII information leakage, financial loss, loss of reputation and loss of loyalty or customer satisfaction (for operators).

As described in clause 6.2, hacking of the original workflow is impersonation, utilizing social engineering attack techniques to hack the authentication process. This hacking attack could be nullified if the authentication is enhanced against impersonation, i.e., the authentication process should be designed and tailored to ensure that the claimed or asserted identity of the smartphone user is indeed the true owner of the SIM card. Therefore, the first move towards risk mitigation should be to examine the resistance of existing technologies to impersonation, choose the one(s) that is or are appropriate and integrate it or them into the authentication process.

In this use case, multifactor authentication has already been used. The user needs to access his or her account first, which means he or she knows his or her own username and password. Then the user needs to input the correct verification code, which is sent to his or her phone number by SMS. This in general means that the user is the one who has the SIM.

A deeper look into these authentication factors reveals a flaw that a password is used as the credential issued to the user by the operator [who acts as the credential service provider (CSP) here]. However, this process of self-registration is in general under LoA1 according to [ITU-T X.1254], which normally happens when an individual accesses a website and, for example, clicks a "new user" button to create a username and password. As explained in clause 6.3, a LoA3 authentication is required in this telecommunication scam use case. Therefore, this flaw comes from inconsistency in LoA procedures and non-conformity to [ITU-T X.1254]. This flaw can be mitigated by employing an LoA3 credential, e.g., some sort of a smartcard to support the digital signature mechanism.

For example, users may be allowed to access the operator's website and click a "new user" button to create a username and password. This is LoA1, and users are allowed to do any LoA1 operations, such as browsing an operator's website for its public policies. However, if a user wants to initiate the SIM card replacement self-service online, which should be under LoA3, then he or she should be requested to provide a universal serial bus (USB) key. This constitutes an LoA3 multifactor authentication, which means that the user not only knows his or her username and password, but also has control of the LoA3 credential, namely the USB key. Please note that during this process of risk mitigation, the nature of the solution is to elevate the user's account to LoA3.

If a USB key is requested when the user initiates a SIM card replacement process, it is apparent that the USB key has already been associated with the user's account. In most cases in current practice, this means that the user has presented him- or herself at the operator's business office to obtain the USB key in person.

The association of the USB key and user account is usually done in the operator's office with the user in person. The binding information shall be kept securely in the operator's database. If the USB key is not delivered to the user in person, a mechanism shall be used to check that the delivery address exists and is legitimately associated with the real user of the SIM. The USB key shall have a specific expiry date based on the operator's policy.

Depending on specific scenarios and considerations, other technologies can be chosen, including biometric identification, such as iris or facial recognition.

6.5 Implementation of SIM card replacement self-service with security

An implementation outline of this SIM card replacement self-service with security is given in Table 6-2.

Table 6-2 – Implementation outline of SIM card replacement self-service

Implementation scenario	Corresponding detailed security considerations
1. Transaction description	SIM card replacement self-service workflow
2. Risk assessment	Lost or stolen smartphone, social engineering attack, impersonation, PII information leakage, financial loss, loss of reputation, loss of loyalty
3. Choose appropriate assurance level	Choice of LoA3 against possible PII information leakage, financial loss, loss of reputation, loss of loyalty, impersonation attack, credential revocation and activation, etc.
4. Select authentication technologies	Digital signature (USB key), multifactor authentication (account and password, SMS, biometric identification including iris recognition or facial recognition), secure storage of user account and PII information
5. Validate the implemented system	No particular risk is created in conjunction with the selected authentication implementation

Table 6-2 – Implementation outline of SIM card replacement self-service

Implementation scenario	Corresponding detailed security considerations
6. Reassess the information system of the implemented system periodically	Set expiration period of USB keys, examine periodically or at certain instances of business, etc.

7 Use case 2: Online shopping

Online shopping has now become very popular, hence various procedures in its service flow face hacking.

Hackers may hack signature generation and verification mechanisms of a third-party payment platform, or post-payment verification procedure of an online shopping provider.

Hackers may also tamper with the price of the merchandise at the beginning of the online shopping procedure, namely the order form generation stage. However, by doing so, the hacking target lies outside the scope of [ITU-T X.1254]; hence that hacking behaviour is not covered in this Supplement.

7.1 Online shopping workflow

Figure 1 is a flow chart of online shopping incorporating a security design. Its payment functionality is realized through a third-party payment platform.

Online shopping starts when a client makes a shopping decision online, continues with generating his or her order form including the shopping parameters for the third-party payment platform for payment, and finally the payment amount is verified by the online shopping service provider. Whether an online shopping transaction completes successfully depends on security being considered throughout and designed into the process.

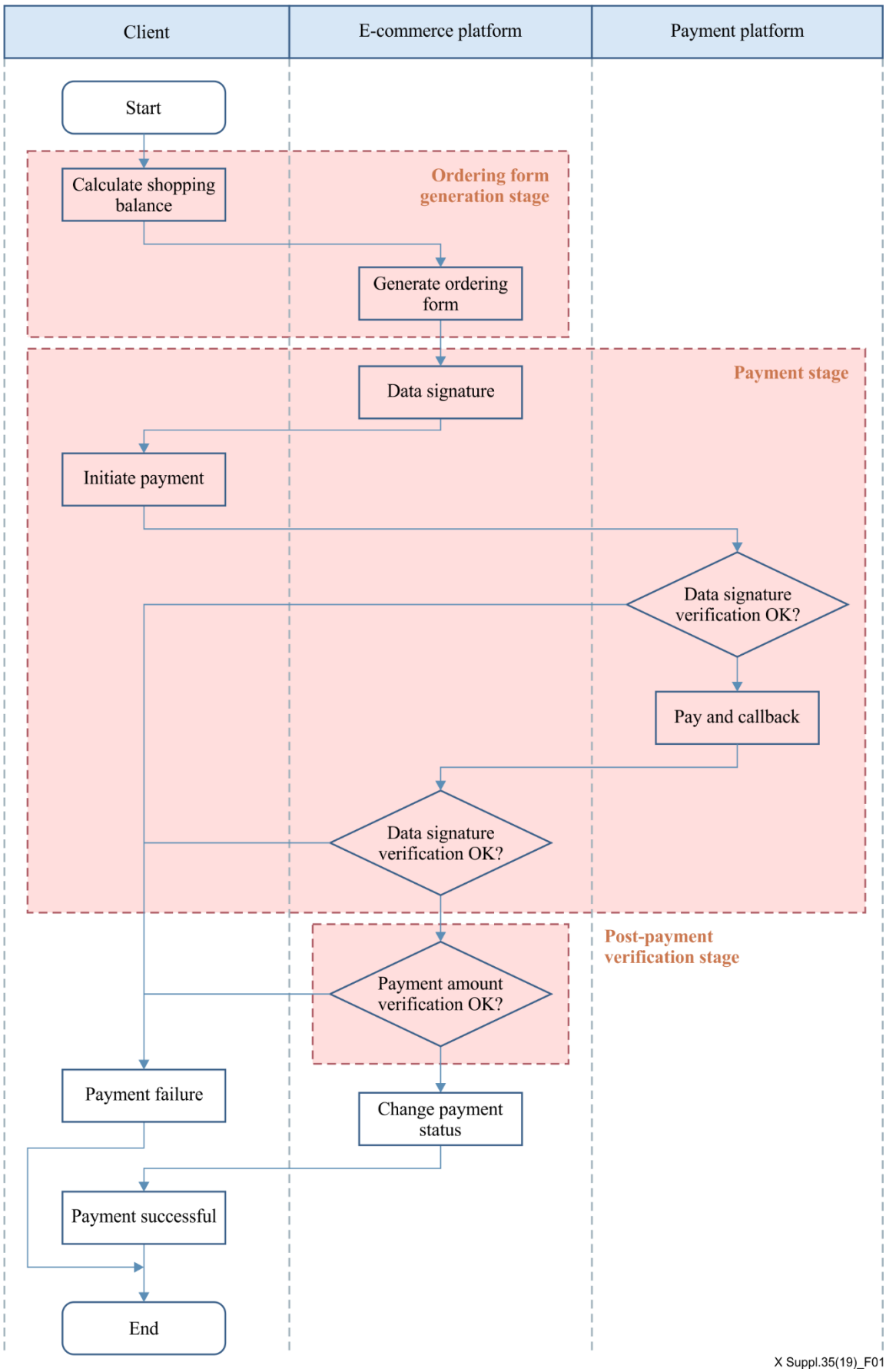

Figure 1 – Online shopping flow chart

In Figure 1, three pink zones indicate three stages of online shopping, namely: order form generation; payment; and post-payment verification.

7.2 Risk assessment

7.2.1 Order form generation stage

At the order form generation stage of an online shopping process, if the payable account is calculated by parameters provided by the front end, e.g., the unit price, there is a high risk that data from the front end might be tampered with, because the cost of hacking in this way is rather low.

Such hacking at the order form generation stage is commonly seen. However, this risk and its mitigation lie outside the scope of this Supplement.

7.2.2 Payment stage

At the payment stage of an online shopping process, access to a third-party payment platform is normally required, and payment security should be ensured by signature and signature verification mechanisms by the third-party payment platform. However, these payment platforms may differ in their signature mechanisms (e.g., message digest algorithm 5 (MD5) and Rivest, Shamir and Adleman (RSA) algorithm public key encryption technology mechanisms). There are risks within the selection and implementation of signature mechanisms.

The steps of implementing an MD5 signature are briefly described as follows.

1. A buyer applies for a payment, i.e., initiates an access to the payment platform.
2. A symmetric key is generated and set on the third-party payment platform (for later signature generation and signature verification procedures).
3. A payment signature is generated by the payment software development kit (SDK) of the third-party payment platform.

The steps of implementing an RSA signature are briefly described as follows.

1. A buyer applies for payment access.
2. A public key infrastructure (PKI) certificate is generated for this client and the client's public key is uploaded to the third-party payment platform. The client's PKI certificate and the private key of the third-party payment platform are stored on the server of the third-party payment platform.
3. A payment signature is generated by the payment SDK of the third-party payment platform.

7.2.3 Post-payment verification stage

Each signature mechanism may have its own risks and its corresponding LoA. It is crucial that an application should correctly assess (evaluate) its risk, and select and implement a corresponding signature mechanism (with the appropriate LoA), so that the risk can be mitigated. If a signature mechanism with a lower LoA is selected and implemented, it is incapable of mitigating the risk.

In the MD5 signature mechanism case, if the symmetric key is leaked, then a hacker may tamper with order form data and generate a signature, as he or she wants. Hence, a reverse verification procedure is necessary to ensure that the amount paid from the payment platform matches the expected payment from the client access side. If a mismatch is detected, the order form is abnormal and should be discarded.

7.3 Risk mitigation approaches

7.3.1 Order form generation stage

As explained in clause 7.2.1, this stage lies outside the scope of this Supplement.

7.3.2 Payment stage

As described in clause 7.2.2, an MD5 signature uses a symmetric cipher, which means that both sides, i.e., user and retailer platforms (including the e-commerce platform and the third-party payment platform shown in Figure 1), use the same key. In other words, security of the symmetric key storage is protected by both the access side (i.e., the user side) and the retailer platform side (including both the e-commerce platform and the third-party payment platform). Payment security is threatened if the key is leaked by either side (external attack or internal leakage).

However, if the RSA signature mechanism is used, which is an asymmetric cipher mechanism, the private key is stored only on the access side, whereas the third-party platform only stores the corresponding public key. In this case, even if the public key is leaked by the third-party platform, payment security is not impaired.

The MD5 and RSA mechanisms are relatively similar in implementation complexity and cost, hence it is recommended that the RSA signature mechanism be used to mitigate risk wherever possible.

7.3.3 Post-payment verification stage

If an MD5 mechanism is used and the symmetric key is leaked, a hacker may tamper with order form data and generate a signature, as he or she wants. Hence, a reverse verification procedure is necessary to ensure that the amount paid from the payment platform matches the expected payment amount from the access side. In these steps, use of signature and verification of signature are also required just as in the payment stage. If a mismatch is detected, the order form is abnormal and should be discarded.

The following steps shall be implemented to mitigate the risk.

1. After successful call-back from a third-party platform, the e-commerce platform queries the amount of the actual payment from the third-party with the ordering serial number.
2. The e-commerce platform gets the amount of the expected payment from the access side (the user side) with the ordering serial number.
3. The e-commerce platform compares the expected and actual amounts of payment, and sees whether they match each other.

7.4 Implementation of online shopping with security

An implementation outline of online shopping with security is given in Table 7-1.

Table 7-1 – Implementation diagram of online shopping

Implementation scenario	Corresponding detailed security considerations
1. Transaction description	Online shopping and online payment realized through third-party online payment platform
2. Risk assessment	1. Form generation stage: does not belong to this use case, omitted 2. Payment stage: accessing the third-party payment platform requires that payment security by signature and signature verification mechanisms of the third-party payment platform be ensured. However, the selection of the signature mechanism may result in different authentication strengths. 3. Post-payment verification stage: the order form data might be tampered with imperceptibly if the symmetric key is leaked

Table 7-1 – Implementation diagram of online shopping

Implementation scenario	Corresponding detailed security considerations
3. Choose appropriate assurance level	Depending on real situations, choose LoA2 or LoA3 authentication assurance for possible PII information leakage, financial loss, loss of reputation, loss of loyalty, impersonation attack, credential revocation and activation, etc.
4. Select authentication technologies	Asymmetric cipher mechanism, mutual authentication, secure storage of user account and PII information
5. Validate the implemented system	No particular risk is created in conjunction with the selected authentication implementation
6. Reassess the information system of the implemented system periodically	Examine periodically or at certain instances of business, including credential suspension, revocation or destruction, etc.

8 Use case 3: Commodity traceback using distributed ledger technology technology

Nowadays, identity theft and data leakage happens more and more often along with progress of digitalization. One characteristic of distributed ledger technology (DLT) is that its historical transaction data are difficult to tamper with. This characteristic can be useful in businesses including retail, banking or insurance. One application is to use DLT for commodity identity verification, i.e., commodity historical transaction data traceback.

8.1 Need for commodity traceback

In the market, fake or inferior products can always be found despite repeated prohibition. These products normally counterfeit good quality and famous brand products. It is difficult: a) for ordinary consumers to distinguish genuine from sham products; b) to trace back the source of fake products. This damages the reputation and brand image of good products.

8.2 Risk assessment

Traditional traceback of commodities requires solutions to the following problems.

1) Traceback of commodities may involve traceback of the production and distribution chains. This increases the number of trust endorsement subjects, making collaboration more difficult.
2) A centralized commodity information system has shortcomings in security; its information is liable to be tampered with, hence the credibility of its information is decreased.
3) A commodity supply chain may have multiple information systems, making crosscheck complicated and difficult.
4) A user's PII is vulnerable to leakage.

8.3 Risk mitigation approaches

The characteristics of DLT include:

– a decentralized system,
– difficult to tamper with,
– lower cost of crosscheck.

These characteristics make DLT suitable for mitigating the risks of traditional commodity traceback issues.

If the characteristics and advantages of DLT were combined, the following benefits could be achieved.

1. Use of DLT will result in distributed records. This change will make all parties in the supply chain more active and sincere in their participation in the commodity traceback system.
2. Mitigation of risk of fake and inferior commodities, as a commodity traceback system can be established and data in this traceback system are difficult to change.
3. Protection of the interests of all parties in the supply chain.

It should be noted that bringing in DLT may introduce new risks in transaction security. For example, a user's PII should be properly handled and access control properly designed and implemented. However, mitigation methods for these new risks lie outside the scope of this Supplement.

8.4 Implementation of commodity traceback with security

An implementation outline of commodity traceback with security is given in Table 8-1.

Table 8-1 – Implementation outline of commodity traceback

Implementation scenario	Corresponding detailed security considerations
1. Transaction description	Online traceback to the source of fake and inferior commodities utilizing DLT; distinguish genuine from sham products
2. Risk assessment	1. Centralized databases, etc. are easier to tamper with. 2. Centralized endorsement of more subjects is more expensive and difficult to realize. 3. As a result, ordinary consumers can easily be spoofed to buy fake or inferior commodities. 4. A fake or inferior commodity is difficult to trace back to its source, making it difficult to distinguish genuine from sham products
3. Choose appropriate assurance level	Depending on real situations, choose LoA2 or LoA3 authentication assurance for possible identity spoofing, financial loss, loss of reputation, loss of loyalty, impersonation attack, credential revocation and activation, etc.
4. Select authentication technologies	Combine an RSA algorithm mechanism with DLT to enhance data security, prevent transaction data from being tampered with, reduce the number of subjects in the supply chain that need to be endorsed, facilitate traceback to product source, facilitate distinction of genuine from sham products
5. Validate the implemented system	Bringing in DLT may also introduce risks in transaction security. A user's PII should be properly handled and access control should be properly designed and implemented
6. Reassess the information system of the implemented system periodically	Examine periodically or at certain instances of business, including credential suspension, revocation or destruction

Bibliography

[b-ITU-T X.1154] Recommendation ITU-T X.1154 (2013), *General framework of combined authentication on multiple identity service provider environments.*

[b-ITU-T X-Sup.33] ITU-T X-series Recommendations – Supplement 33 (2018), *ITU-T X.1231 – Supplement on technical framework for countering telephone service scams*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020