INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2013-2016

STUDY GROUP 17

TD 0235

English only

Original: English

Question(s):	7/17	Geneva, 17-26 April 2013

TD

Source:	Editors
Title:	The baseline text for Recommendation ITU-T X.sap-8, efficient multi-factor authentication mechanisms using mobile devices

Abstract

This TD is the baseline text for Recommendation ITU-T X.sap-8, *efficient multi-factor authentication mechanisms using mobile devices,* which was agreed at the April 2013 SG 17 meeting. It is based on discussion of Contribution 0042 Rev.1.

Contact:	Heung Youl Youm Soonchunhyang University Korea (Republic of)	Tel: +82 41 530 1328 Fax: +82 41 530 1494 Email: hyyoum@sch.ac.kr
Contact:	Keun-ok Kim FSA Korea (Republic of)	Tel: +82 2 6919 9154 Fax: +82 2 6919 9180 Email: kko@fsa.or.kr

Summary

Today, with a wide use of mobile devices, the amount of business transaction through mobile devices is drastically increasing. However, there are many weakness of a single-factor authentication for use in the mobile context, which requires strong authentication mechanisms to meet requirements in terms of the security and convenience. Therefore, there is a strong need for developing multi-factor authentication mechanisms which are applicable to mobile context.

The proposed Recommendation basically provides a multi factor authentication mechanism using mobile devices. It describes a weakness of a single-factor authentication mechanism, a need for multi factor authentication mechanism and various combinations of the multi factor authentication mechanism using mobile devices, and threats for the two-factor authentication mechanism. In addition, security requirements to reduce threats of a single-factor authentication are provided including potential typical multi factor authentication mechanisms. It is to use mobile devices with SIM card capability, and should not exclude use of the virtual SIM cards. Specifically, it is applicable all applications using mobile devices. It will use the framework in the X.sap-4.

Annex B: Baseline document

Draft Recommendation ITU-T X.sap-8

Efficient multi-factor authentication mechanisms using mobile devices

1. Scope

The Recommendation basically provides multi factor authentication mechanisms using mobile devices. It describes a weakness of a single-factor authentication mechanism, a need for multi factor authentication and various combinations of the multi factor authentication mechanism using mobile devices, and threats for the two-factor authentication. In addition, security requirements to reduce threats of authentication mechanism are provided including potential typical multi factor authentication protocols. It is to use mobile devices with SIM card capability, not to exclude the virtual SIM card capability. Specifically, it is applicable all applications using mobile devices. It will use the framework in the X.sap-4.

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 published regularly.

A reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.509] Recommendation ITU-T X.509 (2011), *Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks.*

3. Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 **authentication factor:** Piece of information and process used to authenticate or verify the identity of an entity [ISO/IEC 19790].

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, PIN);
- Something an entity is (e.g., biometric characteristic); or
- Something an entity typically does (e.g., behaviour pattern).

3.1.2 **authentication protocol**: Defined sequence of messages between an entity and a verifier that enables the verifier to corroborate the entity's identity.

3.1.3 **credential** [ITU-T X.1252]**:** Set of data presented as evidence of an asserted or claimed identity and/or entitlements

NOTE – See Annex A for additional characteristics of a credential.

3.1.4 **man-in-the-middle Attack:** Attack in which an attacker is able to read, insert, and modify messages between two parties without their knowledge.

3.1.5 **multifactor authentication**[ISO/IEC 19790]**:** Authentication with at least two independent authentication factors.

3.1.6 **verifier:** Actor that corroborates identity information.

3.1.7 **verify:** Check information by comparing the provided information with previously corroborated information and the binding to the entity.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 **mobile device:** a small, hand-held computing device with a SIM card, typically having a display screen with touch input and/or a miniature keyboard and small weight.

3.2.2 **subscriber identity module**: an integrated chip used mostly in cell phones that operate on the Global System for Mobile Communications (GSM) network, which securely stores the international mobile subscriber identity (IMSI) and the related key used to identify and authenticate subscribers on mobile telephony devices

3.2.3 **virtual SIM card**: A software to emulate a SIM card in a mobile device, which does not require a physical SIM card to connect voice calls and text messaging to a user's mobile device.

4. Abbreviations and acronyms

This Recommendation uses the following abbreviations:

CA	Certification Authority
SFS	Single Factor Authentication
MFS	Multi Factor Authentication
PIN	Personal Identification Number
SIM	Subscriber Identity Module
TFS	Two Factor Authentication

5. Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance. The keywords "**is prohibited from**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed. The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6. Overview of a two-factor authentication mechanism

6.1 Overview

Two-factor authentication is a security process that confirms user identities using two distinctive factors – something they have and something they know. Two-factor authentication uses a mechanism which implements two of the authentication factors and is therefore considered stronger and more secure than the traditionally implemented one factor authentication system.

Two-factor authentication can provide a significant increase in security of authentication system. In the two factor authentication, the password or PIN number can be used in conjunction the use of tokens, smart-cards or even biometrics. The combination of the multi factors will provide companies make sure of the users accessing secure systems of an organization.

A two-factor authentication has been introduced to meet the demand of organizations for providing stronger authentication options to its users. In most cases, a hardware token, e.g., an OTP token or a mobile phone is given to each user for each account. The increasing number of carried tokens and the cost the manufacturing and maintaining them is becoming a burden on both the client and organization. Since many clients carry a mobile phone today at all times, an alternative is to install all the software tokens on the mobile phone. This will help reduce the manufacturing costs and the number of devices carried by the client.

The following are typical benefits of a two-factor system:

- Resistant to single-factor attacks including keystroke monitoring, social engineering, man-in-the middle attacks, network monitoring, password cracking and IT staff abuse;
- Difficult for a user to deny involvement in a transaction because users are held accountable for all actions resulting from a successful user authentication;
- Less likely to lead to fraudulent or unauthorized access to corporate data;
- Easy for end-users to use; and
- Durable and offers a long-term security solution.

Two factor authentications also have disadvantages which include the cost of purchasing, issuing, and managing the tokens or cards. From the customer’s point of view, using more than one two-factor authentication system requires carrying multiple tokens/cards which are likely to get lost or stolen.

The two factor authentication can be regarded as subtype of multifactor authentication, which is authentication with at least two independent authentication factors.

6.2 Single factor authentication

Single-factor authentication (SFA) is the typical authentication mechanism that requires, for example, a user name and password before granting access to the user. Table 1 illustrates typical examples of a single factor authentication.

Table 1 – Typical single-factor authentication

Authentication factor	Examples
Proof of knowledge	Passwords, PIN, Mom's Name, Phone number, etc.
Proof of possession	Smartcards, Tokens, Driver's license, PKI certificates
Inherence proof	Fingerprints, Hand geometry, Facial image, Iris, Retina, DNA, voice, signature patterns

6.3 Multi-factor authentication

In a two-factor authentication system, the user needs to provide two factors, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code and PIN.

Multi-factor authentication (also Two-factor authentication, TFA, T-FA or 2FA) is an approach to authentication which requires the presentation of two or more of the three authentication factors: a knowledge factor ("something the user knows"), a possession factor ("something the user has"), and an inherence factor ("something the user is").

6.4 Basic two factor authentication

This clause specifies simple a two-factor authentication mechanism using a mobile phone.

When a user wants to be authenticated to the web server, a user uses his/her password as the first factor and then a one-time password (something an entity has) as the second authentication factor.

It is assumed that the client and server share secret, Ks, for computing the second authentication factor.

A typical example of authentication protocol may comprise the following steps:

1. The client sends to the server a pair of username and the hashed password, *h(password)*.
2. The server retrieves the hashed value of a user and compares the received hashed password with the retrieved hashed password. In case of successful match, it completes one factor authentication.
3. For the second factor authentication, the client computes S_n, an one-time password at the current session n, from S_{n-1}, an one-time password at the previous session n-1 and the shared secret, Ks, between the server and the client as follows:

   $$S_n = f(K_s, S_{n-1})$$

   The client sends to the server S_n.
4. The server compute S_n' and compares the received S_n and the computed S_n'. In case of a successful match, it completes the second authentication factor.

As long as the token S_{n-1} is adequately secured on the mobile device, proving knowledge of it is sufficient for a second login factor (which the client does by calculating and providing S_n).

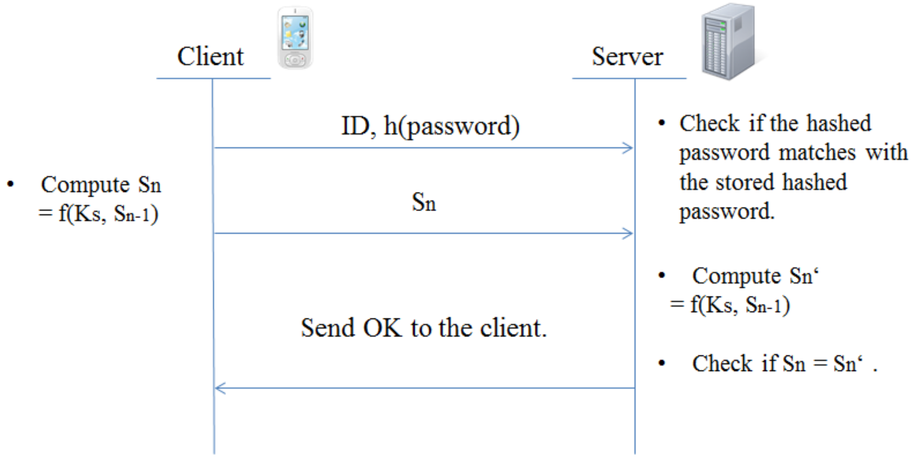
Client
Server
ID, h(password)
• Check if the hashed password matches with the stored hashed password.
• Compute Sn = f(Ks, Sn-1)
Sn
• Compute Sn‘ = f(Ks, Sn-1)
Send OK to the client.
• Check if Sn = Sn‘ .

Figure 6-1: The typical two factor authentication mechanism

6.5 Combination of multi factor authentication mechanisms using mobile phones (devices)

6.6 Threats of multi factor authentication

6.6.1 Key Logging Attacks

Key logging (more often called *keylogging* or "keyloggers") is the action of recording (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored and recoding. It is sometimes implemented in Software that is run on the mobile devices.

6.6.2 Lost or Stolen Mobile Device& List of OTPs

The mobile devices are getting most favorite target for theft since it contains credential information that may lead to financial gains. A malicious attacker could steal the cell phone and attempt to login to various user accounts.

6.6.3 Shoulder Surfing

Shoulder surfing indicates attacker’s ability to obtain all or part of a user's credentials by taking a brief look at the information provided by the user during authentication.

6.6.4 Phishing/active/passive Man-in-the-Middle Attack

Man-in-the-middle attack is a special type of social engineering in which the attacker resides in between the user and the intended service provider and tries to resemble the behavior of the original service provider in order to fool the user into revealing the required credentials.

6.6.5 Session Hijacking and Parallel Session Hijacking

In a session hijacking attack, malware or an attacker can take over a session already opened by the user, and use the stored information in the session to perform other transactions or alter the transactions.

6.6.6 Denial of Service Attack

Depending on the method of communication between the mobile device and the personal computer, a DoS attack might be possible to carry out.

7. Formal Analysis of the Security Protocol Security requirements for multi factor authentication mechanisms

7.1 General requirement

- The multifactor authentication mechanisms should be designed to be resistant to threats described in clause 6.6.

8. Efficient multi factor authentication mechanisms using mobile devices

Bibliography

1. Fadi Aloul, Syed Zahidi, Wassim El-Hajj, “Two Factor Authentication Using Mobile Phones,” http://www.aloul.net/Papers/faloul_aiccsa09.pdf
2. Roger Elrod, Two-Factor Authentication, East Carolina University, 2005, http://www.infosecwriters.com/text_resources/pdf/Two_Factor_Authentication.pdf
3. Andrew Kemshall, Phil Underwood, Options for Two Factor Authentication, July, 2007.
4. 2-Factor authentication for mobile applications, DSWISS Ltd., 2010, http://pd.zhaw.ch/hop/528326154.pdf
5. Aladdin Secure SafeWord 2008. Available at *http://www.securecomputing.com/index.cfm?skey=1713*
6. B. Schneier, “Two-Factor Authentication: Too Little, Too Late,” in *Inside Risks 178*, *Communications of the ACM*, 48(4S)**,** April 2005.
7. D. Ilett, “US Bank Gives Two-Factor Authentication to Millions of Customers,” 2005. Available at *http://www.silicon.com/financialservices/0,3800010322,39153981,00.htm*
8. Nima Kaviani, Kirstie Hawkey, Konstantin Beznosov, “A Two-factor Authentication Mechanism Using Mobile Phones,” Technical report LERSSE-TR-2008-03, University of British Columbia, August, 2008. http://lersse-dl.ece.ubc.ca/record/163/files/163.pdf
9. iKey™ 1000 Series – Smart Devices for Two-Factor Authentication, Rainbow Technologies, Inc.
