

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1151

(11/2007)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Telecommunication security

**Guideline on secure password-based
authentication protocol with key exchange**

ITU-T Recommendation X.1151



ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	X.1000–

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

ITU-T Recommendation X.1151

Guideline on secure password-based authentication protocol with key exchange

Summary

A secure password-based authentication protocol with key exchange is a kind of authentication protocol with authenticated key exchange using a human-memorable password. It is very simple and easy to implement as well as easy to use; no need for other infrastructure, e.g., PKI. A secure password-based authentication protocol with key exchange (SPAK) becomes very important, since a variety of usage cases in many applications will emerge in the near future. In addition, SPAK provides both user authentication and strong key exchange with weak password, i.e., the subsequent communication session can be protected by a shared secret during the authentication procedure.

ITU-T Recommendation X.1151 is intended to identify a set of requirements for password-based authentication protocols and define the guideline for selecting the most suitable password authentication protocol by presenting the criteria for choosing an optimum SPAK protocol for applications. SPAK can also be used in a wide variety of applications wherein pre-shared secrets based on the weak password exist.

Source

ITU-T Recommendation X.1151 was approved on 13 November 2007 by ITU-T Study Group 17 (2005-2008) under the ITU-T Recommendation A.8 procedure.

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

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation 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 Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. 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/>.

© ITU 2008

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

	Page
1 Scope	1
2 References.....	1
3 Terms and definitions	1
4 Abbreviations and acronyms	3
5 Conventions	3
6 Secure password-based authentication protocol with key exchange (SPAK).....	3
6.1 Problems of plaintext password-based authentication	4
6.2 Operational procedure of SPAK.....	4
6.3 Basic characteristics of SPAK.....	4
7 Requirements for SPAK	4
7.1 Framework requirement	4
7.2 Protocol requirement	5
8 Criteria for choosing a suitable SPAK.....	6
Annex A – SPAK framework requirements	8
Appendix I – Comparison of existing SPAKs in terms of performance and underlying PKC	9
Appendix II – Comparison of existing SPAK protocols in terms of several requirements	10
Bibliography.....	11

ITU-T Recommendation X.1151

Guideline on secure password-based authentication protocol with key exchange

1 Scope

This Recommendation is intended to identify a set of requirements for secure password-based authentication protocols with key exchange (SPAK) and define the guidelines for selecting a most suitable SPAK among various secure password authentication protocols by presenting the criteria for choosing an optimum SPAK protocol for applications. SPAK can also be used in a wide variety of applications wherein pre-shared secrets based on the weak password exist.

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] ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications.*
- [ITU-T X.1035] ITU-T Recommendation X.1035 (2007), *Password-authenticated key exchange (PAK) protocol.*
- [ITU-T X.1111] ITU-T Recommendation X.1111 (2007), *Framework of security technologies for home network.*
- [ITU-T X.1121] ITU-T Recommendation X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications.*

3 Terms and definitions

This Recommendation defines the following terms:

3.1 active attack: This attack involves the modification or injection of information listening.

3.2 dictionary attack: This is an attack wherein an attacker collects a database of commonly used words and passwords that can be encrypted using all possible salts and compares its database of encrypted terms against the encrypted passwords found in a password file on the system. If a match is found, the actual password is known, and access is gained. The dictionary attack can be grouped into two categories: online dictionary attack and offline dictionary attack. In the online dictionary attack, the attacker repeatedly attempts authentication with the server using guessed passwords until he or she succeeds. The online dictionary attack can be detected or prevented by counting the number of access failures. On the other hand, the offline dictionary attack is normally performed by someone posing as a legitimate user to gather information or one eavesdropping on messages between two parties during a successful protocol run. The attacker uses the captured packets to guess the password.

3.3 identity theft: Identity theft and identity fraud are the terms used to refer to all types of crime wherein a person wrongfully obtains and uses another person's personal data in a fraudulent or deceptive manner and usually for economic gain.

3.4 man-in-the-middle attack: This is an attack wherein an attacker intercepts the public or cryptographic keys being exchanged by two entities and substitutes his/her own public key to impersonate the recipient. This successful attack results in the compromise of the cryptosystem or SPAK.

3.5 mutual authentication: This means that a client is able to authenticate a server, which is also able to authenticate a client. In other words, one of two parties proves to the other that it knows the password.

3.6 passive attack: This is an attack that involves listening, i.e., eavesdropping, without modification or injection of information.

3.7 perfect forward secrecy: In cryptography particularly in a key-establishment protocol, the condition wherein the compromise of a session key or a long-term private key after a given session does not cause the compromise of any of the earlier sessions. In the context of SPAK, this means that the disclosure of the password does not result in revealing the previously recoded encrypted conversation by deriving such session key.

3.8 pharming: Whereas phishing involves redirecting the website's traffic to another forged website, pharming attacks by compromising the domain name system (DNS) server. Specifically, pharming modifies into another addresses the correct IP addresses that corresponds to a domain name in the DNS server; thus redirecting the user to a hacker's forged website when he/she is asked to enter the company's Web address.

3.9 phishing: This refers to the act of sending an email to a user, falsely claiming to be an established legitimate enterprise in an attempt to con the user into surrendering private information that will be used for identity theft. The email directs the user to a website where he/she is asked to update personal information such as passwords and credit card, social security, and bank account numbers, information that the legitimate organization already has. Note, however, that the website is bogus, set up only to steal the user's information.

3.10 plaintext-equivalent SPAK: This is a type of SPAK wherein the server stores the plaintext of the user's password or password-equivalent information. This SPAK is called symmetric SPAK.

3.11 secure password-based authentication protocol with key exchange: In this simple authentication protocol, using a memorable password between a client and the server results in mutual authentication and shared secret that can be used as session key for the next session.

3.12 server-compromised attack: This is an attack wherein an attacker obtains verifier information from the server and launches a dictionary attack on the password file.

3.13 server-compromised dictionary attack: In the case of a server-compromised attack, the password may be obtained by performing a dictionary attack on the compromised verifier. If the server uses a tamper-free token such as smart card to store additional information or other cryptographic methods to prevent a server-compromised attack, a password can still not be derived even if a dictionary attack is launched on the verifier.

3.14 verifier: The verifier is the information computed from the password. Whereas computing the verifier from the password is easy, the reverse is infeasible in polynomial time. The verifier is used in the server to prove that a client knows the password. It is similar to a public key in public-key cryptography. On the other hand, the password looks like a private key but has limited entropy and relies on the memory of the user. The verifier must be kept confidential by the server.

3.15 verifier-based SPAK: This is a type of SPAK wherein the server stores only the verifier of a password. The password is different from the verifier of a password. This SPAK is called asymmetric SPAK.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

DH	Diffie-Hellman
DNS	Domain Name System
PIN	Personal Identification Number
PKC	Public-Key Cryptography
PKI	Public-Key Infrastructure
SPAK	Secure Password-based Authentication protocol with Key exchange
SSL	Secure Socket Layer

5 Conventions

None.

6 Secure password-based authentication protocol with key exchange (SPAK)

The techniques for user authentication are based on one or more of the following categories:

- 1) What you know;
- 2) What you are; or
- 3) What you have.

Passwords or personal identification number (PIN)s are examples of the first category. The biometric technique falls into the second category. Identification tokens such as smart cards fit in the third category. Two entities sharing a password and communicating over an insecure network want to authenticate each other and agree on a large session key to be used for protecting their subsequent communication. This is called a password-authenticated key exchange protocol. If one of the entities is a client, and the other, a server, then this can be regarded as a problem in the area of remote user access.

A secure password-based authentication protocol with key exchange is defined as a simple authentication protocol wherein using memorizable password between a client and the server results in mutual authentication and shared secret that can be used as session keys for the next session.

In general, SPAK uses the DH (Diffie-Hellman) algorithm to share the session key and the hash algorithm to blind the public DH parameters using a password. Therefore, the underlying cryptography may generally be DH public-key algorithm.

SPAK can be grouped into two categories: plaintext-based SPAK and verifier-based SPAK. In plaintext-based SPAK, a symmetrical secret is shared between a client and a server; in a verifier-based SPAK, however, the secret of a server is totally different from that of a client. In other words, a server only stores the verifier derived from a password; an attacker will have difficulty obtaining a password from the verifier of a server.

There is a need to study password authentication protocols, identify the vulnerabilities in environments using the password authentication protocol, and set the criteria for selecting an optimal password authentication protocol among various existing authentication protocols. Moreover, the guidelines for an optimal secure password-based authentication protocol with key exchange help a designer or a user to develop his/her authentication scheme efficiently and easily.

6.1 Problems of plaintext password-based authentication

Most application protocols still use a password-based authentication protocol. One example is an ID/password authentication method protected by a secure tunnel such as secure socket layer (SSL). Most of the solutions such as tokens, smart cards, etc., are neither cost-effective nor convenient nor available. In fact, phishing and pharming become real threats for most of the Internet applications. These types of threats can be protected by mutual authentication that can be provided by a secure password-based authentication protocol. Identity theft is another threat. Therefore, a secure password-based authentication protocol with key exchange needs to consider protection from these kinds of attacks. This contribution identifies the requirements for a strong password authentication protocol to provide a selection guide for a designer or a user of a home network.

6.2 Operational procedure of SPAK

A server and a client are assumed to share a password or password-related information before performing a strong authentication protocol. A client remembers the password, and a server secures a password itself or password-related information, e.g., hashed value of a password. A client is assumed to be connected to the server via an open network or an insecure network, e.g., Internet, which is very vulnerable to various threats. In SPAK protocol, system parameters such as prime numbers and strong one-way hash function are made public. The following describes how the secure password-based authentication protocol with key exchange generally works:

- The client enters a password.
- The server and a client swap a public key of a chosen length.
- The server authenticates a client; a client also authenticates a server.
- As a side effect, a server and a client derive a shared secret that can be used as a cryptographic key in the next session.

6.3 Basic characteristics of SPAK

The following are the basic characteristics of SPAK protocol:

- Should provide mutual authentication without exchanging plain-text password.
- Should offer minimal burden on the client and the server.
- No need for additional hardware tokens or infrastructure such as PKI certificates.

The secure session procedure follows a strong password authentication protocol, i.e., the secret shared between the client and the server may be used to protect the session.

7 Requirements for SPAK

Authentication is a process of verifying that the client is who he/she claims to be. This process is carried out between a client and the server. There are two entities involved in the strong password authentication protocol.

7.1 Framework requirement

The framework requirement of a secure password-based authentication protocol with key exchange is presented in Annex A.

7.2 Protocol requirement

In this clause, the requirements for secure password-based authentication protocols with key exchange are identified by listing a set of relevant vulnerabilities and the requirements that must be met by all protocols. Afterward, the criteria for providing a selection guideline are identified to provide a designer with guidelines for selecting an optimal password authentication protocol among many existing password authentication protocols.

7.2.1 Vulnerabilities

This clause describes the vulnerabilities in a strong password authentication protocol. SPAK should offer protection against these vulnerabilities. Ideally, any protocol claiming to meet the requirements listed in this Recommendation should explicitly indicate how (or whether) it plans to offer protection for each of these vulnerabilities.

- A passive attacker can eavesdrop on all packets on the network, launch an online dictionary attack at that moment, and carry out a dictionary attack later by using the passive attack.
- An attacker can attempt to modify the message in transit by using the active attack.
- An attacker can fabricate or forge the message on behalf of a legitimate client.
- An attacker may try to masquerade as an authentication server in an attempt to make a client reveal information online and consequently allow for a dictionary attack later.
- An attacker may attempt to get a client to decrypt a chosen "ciphertext" and to make use of the resulting plaintext; at this time, the attacker may be able to launch a dictionary attack, e.g., if the plaintext resulting from the "decryption" of a random string is used as a DSA private key.
- An attacker can try to pretend as a client in an attempt to get a server to reveal information that allows for a dictionary attack later.
- An attacker can convince a server that successful login has occurred, even if this is not the case.
- An attacker can force a password change targeting a known (or "weak") password.
- An attacker may attempt to launch a man-in-the-middle attack.
- The user enters a password instead of a name.
- An attacker may attempt various denial-of-service attacks against a server.
- An attacker may attempt to launch server-compromised attacks.
- An attacker may attempt to launch server-compromised dictionary attacks.

7.2.2 Protocol requirements of SPAK

There are several requirements that must apply to the strong password authentication protocol to enable it to offer protection against the vulnerabilities described in clause 7.2.1.

- The protocol offers perfect forward secrecy.
- The protocol provides mutual authentication based on a pre-shared, human-memorable password.
- The protocol resists a replay attack.
- The protocol does not find the shared password from the compromised session key of a previous session. Such an attack is known as the Denning-Sacco attack.
- The protocol protects against a man-in-the-middle attack. In other words, it is impossible for an attacker to impersonate the client or the server.
- The protocol protects against an online dictionary attack.

- The protocol supports a range of cryptographic algorithms including symmetric and asymmetric algorithms, hash algorithms, and MAC algorithms.
- The protocol can ensure the authenticity of the server.
- The protocol can ensure the authenticity of the client.
- Client-initiated authentication information (e.g., password) change must be supported.
- The protocol prevents any leakage of the information viewed during a successful run.
- The protocol protects against an offline dictionary attack.
- The protocol protects against a server-compromised attack. In other words, an attacker compromising the password verification-related file from the server can neither impersonate the user without launching a dictionary attack on the password file nor derive old session keys from such compromised password.
- The protocol protects against a server-compromised dictionary attack.
- The protocol can be a verifier-based SPAK or a plaintext-equivalent SPAK.
- The protocol should be simple or easy to implement to promote widespread adoption and to minimize security flaw.
- The protocol requires minimal client configuration.
- The protocol requires minimum storage and minimum computation particularly minimum exponentiation operation, which requires considerable computational complexity.
- Sharing of secrets across multiple servers is possible, provided the penetration of some servers does not expose the private parts of a credential ("m-out-of-n" operation, $n > m$).

8 Criteria for choosing a suitable SPAK

A strong password authentication can be compared in terms of the volume of communication data, total volume of cryptographic computations, the number of generating random numbers, the number of protocol rounds, or value of system parameter. In general, the total volume of cryptographic computations depends mainly on the number of modular exponentiations, which require more computational time than other arithmetic operations such as addition or multiplication.

The criteria for choosing a specific SPAK depends on the requirements of a designer of an application. If SPAK is used to convey a critical message for applications, e.g., credential transfer server and electronic fund transfer, the level of SPAK to be selected should be very high. On the other hand, the level of SPAK should be low if it is used to transfer information for less important applications such as file transfer and web application.

Therefore, SPAK may be grouped into three categories: High-level SPAK (Type C SPAK), medium-level SPAK (Type B SPAK), and basic SPAK (Type A SPAK). The criteria for selecting a suitable type of SPAK are listed in Table 1.

The three types of SPAK may be classified according to the level of security requirements. Type A SPAK should satisfy some of the basic requirements such as perfect forward secrecy, mutual authentication, replay attack, man-in-the middle attack, and Denning-Sacco attack including a range of basic cryptographic algorithm support such as various hash functions as well as the authenticity of server, authenticity of client, client-initiated authentication information (e.g., password) change, and online dictionary attack. Note that these same requirements are satisfied by symmetrical SPAKs. On the other hand, Type B SPAK should satisfy all the requirements of Type A SPAK as well as additional requirements such as a server-compromised dictionary attack. This additional requirement is designed to protect from a server-compromised attack. Type C SPAK must satisfy all the requirements of Type B and one additional requirement such as a server-compromised dictionary attack. This additional requirement is intended to strengthen Type B SPAK by protecting against the server-compromised dictionary attack wherein authentication information is not

compromised when the server is compromised by the attacker. Type C SPAK can be implemented using the tamper-free module, e.g., smart card and trusted module.

An application satisfying the very strict security requirements is required to use the Type C SPAK to protect the authentication system from a server-compromised attack.

As shown in Table 1, "M" denotes a mandatory requirement for a certain type of SPAK; "S" means that the specific requirement should be satisfied by a certain type of SPAK. Finally, "O" denotes an optional requirement for a certain type of SPAK.

Table 1 – Criteria for evaluating a specific level of SPAK

	Type A SPAK	Type B SPAK	Type C SPAK
Perfect forward secrecy	M	M	M
Mutual authentication	M	M	M
Resistance to Replay attack	M	M	M
Resistance to Man-in-the-middle attack	M	M	M
Resistance to Denning-Sacco attack	M	M	M
Resistance to Online dictionary attack	M	M	M
Range of basic cryptographic algorithm support such as various hash functions	M	M	M
Authenticity of server	M	M	M
Authenticity of client	M	M	M
Client-initiated authentication information (e.g., password) change	M	M	M
Protection against offline dictionary attack	M	M	M
Protection against server-compromised attack	S	M	M
Verifier-based SPAK	S	M	M
Protection against server-compromised dictionary attack	S	S	M
Simplicity	S	S	S
Minimal client configuration	S	S	S
Minimum storage and minimum computation	S	S	S
Sharing of authentication information across multiple servers	O	O	O
NOTE – M: must; S: should; O: may.			

Annex A

SPAK framework requirements

(This annex forms an integral part of this Recommendation)

This annex describes the requirements that should be met by the SPAK protocol compared to requirements that should be met by a specific protocol using the framework.

In general, SPAK runs at the application level. There is a wide range of deployment options for SPAKs. In many of these cases, being able to reuse an existing user authentication scheme helps, e.g., where passwords have been previously established, reusing them may be more secure than trying to manage a whole new set of passwords. Different devices may also limit the possible types of user authentication scheme, e.g., not all mobile devices are practically capable of carrying out asymmetric cryptography.

The SPAK framework must allow for protocols supporting various secure password-based authentication protocols with different capabilities.

Different devices allow for different transport layer possibilities, e.g., current mobile devices may not support TCP. Therefore, the framework has to be transport-"agnostic".

The SPAK framework must allow the use of different transports. For instance, there are two typical transport methods: TCP and UDP.

Appendix I

Comparison of existing SPAKs in terms of performance and underlying PKC

(This appendix does not form an integral part of this Recommendation)

Table I.1 presents the comparison of SPAKs in terms of several factors such as the number of protocol rounds, volume of communication data, the number of generating random numbers, total volume of cryptographic computations, or value of system parameter. Table I.2 shows the comparison of existing SPAKs in terms of basic requirements such as perfect forward secrecy, online dictionary attack, server-compromised attack, and server-compromised dictionary attack.

Table I.1 – Comparison of existing SPAKs in terms of communication and complexity efficiency

		DH-EKE	SPEKE	SRP	PAK	AMP
Number of protocol rounds		4	4	4	3	4
Volume of communication data [large block]		2	2	2	2	2
Numbers of generating random numbers	Client	1	1	1	1	1
	Server	1	1	1	1	1
Volume of cryptographic computations, exponentiation operation	Client	2	2	3	2	2
	Server	2	2	3	2	2
NOTE – A large block means that the length of the exchanged message is equal to that of a large prime number, e.g., 1024 bits. The numbers may vary for the possible variants of the basic scheme.						

Table I.2 – Comparison of existing SPAKs in terms of the underlying PKC

	DH-EKE	SPEKE	SRP	PAK	AMP
Underlying PKC	DH	DH	DH	DH	DH

Appendix II

Comparison of existing SPAK protocols in terms of several requirements

(This appendix does not form an integral part of this Recommendation)

The following existing SPAK protocols have been identified as need to be studied:

- SRP (Secure Remote Password protocol) [b-IETF RFC 2945]
- PAK (Password-Authenticated Key exchange) [ITU-T X.1035]
- SPEKE (Simple Password-authenticated Exponential Key Exchange) [b-Jablon]
- DH-EKE (DH-based Encrypted Key Exchange) [b-BM]
- AMP (Authentication and Key Agreement via Memorable Password) [b-Kwon]

A detailed comparison is shown in Table II.1. The comparison items are selected from the items of SPAK's general requirements. In this table, a symbol "Y" means that a specific SPAK meets the specific requirement; the symbol "-" means that such requirement is not met.

Table II.1 – Criteria for evaluating a specific level of SPAK

	DH-EKE	SPEKE	SRP	PAK	AMP
Perfect forward secrecy	Y	Y	Y	Y	Y
Mutual authentication	Y	Y	Y	Y	Y
Resistance to Replay attack	Y	Y	Y	Y	Y
Resistance to Man-in-the-middle attack	Y	Y	Y	Y	Y
Resistance to Denning-Sacco attack	Y	Y	Y	Y	Y
Resistance to Online dictionary attack	Y	Y	Y	Y	Y
Range of basic cryptographic algorithm support such as various hash functions	Y	Y	Y	Y	Y
Authenticity of server	Y	Y	Y	Y	Y
Authenticity of client	Y	Y	Y	Y	Y
Protection against Offline dictionary attack	Y	Y	Y	Y	Y
Protection against Server-compromised attack	–	–	Y	–	Y
Verifier-based SPAK	–	–	Y	–	Y
Protection against Server-compromised dictionary attack	–	–	–	–	Y

Bibliography

- [b-Wu] WU (T.): The secure remote password protocol, *Internet Society Symposium on Network and Distributed System Security*, 1998.
- [b-BM] BELLOVIN (S.), MERRITT (M.): Encrypted key exchange: password-based protocols secure against dictionary attacks, *Proc. IEEE Comp. Society Symp. on Research in Security and Privacy*, pp. 72-84, 1992.
- [b-Kwon] KWON (T.): Authentication and Key Agreement via Memorable Password, *IACR*, e-print, August 2000.
- [b-Jablon] JABLON (David P.): Strong password-only authenticated key exchange, *ACM Computer Communications Review*, October 1996.
- [b-IETF RFC 3157] IETF RFC 3157 (2001), *Securely Available Credentials – Requirements*.
- [b-IETF RFC 2945] IETF RFC 2945 (2000), *SRP Authentication and Key Exchange System*.
- [b-IETF RFC 3767] IETF RFC 3767 (2004), *Securely Available Credentials Protocol*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
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	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
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 and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems