International Telecommunication Union

# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

# X.1035

(02/2007)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

# Password-authenticated key exchange (PAK) protocol

ITU-T Recommendation X.1035

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.1035

# Password-authenticated key exchange (PAK) protocol

## Summary

ITU-T Recommendation X.1035 specifies a protocol, which ensures mutual authentication of both parties in the act of establishing a symmetric cryptographic key via Diffie-Hellman exchange. The use of Diffie-Hellman exchange ensures the *perfect forward secrecy* – a property of a key establishment protocol that guarantees that compromise of a session key or long-term private key after a given session does not cause the compromise of any earlier session. With the proposed authentication method, the exchange is protected from the *man-in-the-middle* attack. The authentication relies on a pre-shared secret (e.g., password), which is protected (i.e., remains unrevealed) to an eavesdropper preventing an off-line dictionary attack. Thus, the protocol can be used in a wide variety of applications where pre-shared secrets based on the possibly weak password exist.

## Source

ITU-T Recommendation X.1035 was approved on 13 February 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. 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/.

# CONTENTS

**Page**

## Introduction

The *Diffie-Hellman* key exchange, although it provides the *perfect forward secrecy,* is vulnerable to the *man-in-the-middle* attack, as is well known. There are several methods of mitigating such attacks; some of them rely on public key cryptography, while others rely on shared secrets (passwords). This Recommendation specifies a protocol of the latter kind.

Specifically, with the proposed authentication method, the exchange is protected from the *man-in-the-middle* attack. The authentication relies on a potentially weak pre-shared secret, which is concealed (i.e., remains unrevealed) from an eavesdropper preventing an off-line dictionary attack. Thus, the protocol can be used in a wide variety of applications where pre-shared secrets (such as password-based ones) are employed.

PAK advantages are listed below:

– Provides strong key exchange with weak passwords;

– Foils the man-in-the-middle attack;

– Provides explicit mutual authentication;

– Ensures perfect forward secrecy.

Additional information on PAK is provided in the documents that are listed in the Bibliography.

# ITU-T Recommendation X.1035

# Password-authenticated key exchange (PAK) protocol

## 1 Scope

This Recommendation provides description of the password-authenticated key exchange (PAK) protocol that meets the following requirements:

– Provides mutual authentication based on a pre-shared password;

– Provides protection against a man-in-the-middle and against offline dictionary attacks.

This Recommendation also provides guidance on the selection of the parameters for Diffie-Hellman key exchange.

## 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.

[TIA 683-D] TIA Standard TIA-683-D (2006), *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*.

## 3 Definitions

*None*.

## 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

| | |
|---|---|
| PAK | Password-Authenticated Key Exchange |
| PW | Password |
| SHA | Secure Hash Algorithm |
| WLAN | Wireless Local Area Network |

## 5 Conventions

The following conventions are used in this Recommendation:

- *a mod b* denotes the least non-negative remainder when *a* is divided by *b*;
- $H_i(u)$ denotes an agreed-on hash function (e.g., based on *SHA-1*) computed over a string *u*, where $i = 1, 2, 3, ...$ The various $H_i()$ act as independent random functions. The use of different random functions in PAK protocol is recommended in order to strengthen the protocol's security.
- $s|t$ denotes concatenation of the strings *s* and *t*.

## 6 Protocol description

Diffie-Hellman key agreement requires that both the sender and recipient of a message create their own secret random numbers and exchange the exponentiation of their respective numbers. By raising the exchanged value with its secret random number, both parties can compute the same shared secret Diffie-Hellman key.

There are two communicating parties in PAK, *A* and *B*, which share a secret password *PW*. The global Diffie-Hellman publicly known constants, a prime *p* and a generator *g* are carefully selected so that

1) a safe prime *p* is large enough to make the computation of discrete logarithm infeasible; and

2) powers of *g* modulo *p* cover the entire range of *p*-1 integers from 1 to *p*-1.

Initially, *A* selects a secret exponent $R_A$ and computes $g^{R_A} \bmod p$; *B* selects a secret exponent $R_B$ and computes $g^{R_B} \bmod p$. For efficiency purposes, short exponents could be used for $R_A$ and $R_B$ provided they have a certain minimum size. In the following steps, all multiplication operations should be done mod *p*, so all values that are being exchanged between the communicating parties are not larger than *p*. Consequently, all division operations should also be done mod *p*.

Then:

1) *A* initiates the exchange by picking a random $R_A$ and sending the quantity $X = H_1(A|B|PW) \cdot (g^{R_A} \bmod p)$ to *B;*

2) *B*, upon receiving that quantity, verifies that X is not a zero and then divides it by $H_1(A|B|PW)$ to recover $g^{R_A} \bmod p$. Then *B* picks a random $R_B$ and computes $S_1 = H_3(A|B|PW|\frac{X}{H_1(A|B|PW)}|g^{R_B} \bmod p|\left\{\left(\frac{X}{H_1(A|B|PW)}\right)^{R_B} \bmod p\right\})$ and $Y = H_2(A|B|PW) \cdot (g^{R_B} \bmod p)$. *B* sends to *A* a message that contains both quantities $S_1$ and *Y*.

3) Upon receiving that message and verifying that *Y* is not zero, *A* can authenticate *B* by recovering what should be $g^{R_B} \bmod p$ and computing $S_1$ itself. If the result is equal to the received value, *A* computes the key $K = H_5(A|B|PW|g^{R_A} \bmod p|\frac{Y}{H_2(A|B|PW)}|\left\{\left(\frac{Y}{H_2(A|B|PW)}\right)^{R_A} \bmod p\right\})$ . To authenticate itself and complete the exchange, *A* also computes the quantity $S_2 = H_4(A|B|PW|g^{R_A} \bmod p|\frac{Y}{H_2(A|B|PW)}|\left\{\left(\frac{Y}{H_2(A|B|PW)}\right)^{R_A} \bmod p\right\})$ and sends it to *B*.

4) *B* authenticates *A* by computing $S_2$ itself and checking it against the value received from *A*. If both values are the same, *B* also computes the key $K = H_5(A|B|PW|\frac{X}{H_1(A|B|PW)}|g^{R_B} \bmod p|\left\{\left(\frac{X}{H_1(A|B|PW)}\right)^{R_B} \bmod p\right\})$.

If any of the above verifications fails, the protocol halts; otherwise, both parties have authenticated each other and established the key.

The summary of the above steps is illustrated by Figure 1, where *P* denotes *A*|*B*|*PW* (*P* = *A*|*B*|*PW)* and some formulas have been simplified.

| Party A | | Party B |
|---|---|---|
| $X = H_1(P)\cdot(g^{RA} \bmod p)$ | $\xrightarrow{X}$ | Verify that received value is not 0<br>$\frac{H_1(P)\cdot(g^{RA} \bmod p)}{H_1(P)} = g^{RA} \bmod p$ |
| $S\ _1 = H_3(P \mid g^{RA} \bmod p \mid g^{RB} \bmod p \mid g^{R_AR_B} \bmod p)$<br>Calculate $S_1$ and verify that it is equal to the received value for $S_1$ from *B* | $\xleftarrow{S_1, Y}$ | $S_1 = H_3(P \mid g^{RA} \bmod p \mid g^{RB} \bmod p \mid g^{R_AR_B} \bmod p)$<br>$Y = H_2(P)\cdot(g^{RB} \bmod p)$ |
| $S_2 = H_4(P \mid g^{RA} \bmod p \mid g^{RB} \bmod p \mid g^{R_AR_B} \bmod p)$ | $\xrightarrow{S_2}$ | $S\ _2 = H_4(P \mid g^{RA} \bmod p \mid g^{RB} \bmod p \mid g^{R_AR_B} \bmod p)$<br>Calculate $S_2$ and verify that it is equal to the received value for $S_2$ from *A* |
| $K = H_5(P \mid g^{RA} \bmod p \mid g^{RB} \bmod p \mid g^{R_AR_B} \bmod p)$ | | $K = H_5(P \mid g^{RA} \bmod p \mid g^{RB} \bmod p \mid g^{R_AR_B} \bmod p)$ |

**Figure 1 – Description of the PAK protocol**

## 7 Security considerations

This clause considers security aspects of PAK. Specifically, it provides guidance on the selection of the Diffie-Hellman parameters.

Only previously agreed-upon values for parameters *p* and *g* should be used in the PAK protocol. This is necessary to protect against an attacker sending bogus *p* and *g* values and thus tricking the other communicating party in improper Diffie-Hellman exponentiation. The use of the parameters *p* and *g* that do not meet the requirements described in this Recommendation may result in a compromise of the password. A proper 1024-bit value for *p* and an appropriate value for *g* are published in [TIA 683-D].

In addition, if short exponents are used for Diffie-Hellman parameters $R_A$ and $R_B$, then they should have a minimum size of 384 bits (assuming 128-bit session keys are used) as also required in [TIA 683-D].

The independent random functions $H_1$ and $H_2$ should have output 1152 bits each, assuming prime *p* is 1024 bits long and session keys *K* are 128 bits long. The random functions $H_3$, $H_4$, and $H_5$ should have output 128 bits.

EXAMPLE: The use of the [b-FIPS 180-2] SHA-1 hashing function could be recommended for instantiation of the random functions $H_i()$ as described in [b-TIA 1050]. However, it should be noted that NIST is encouraging the use of SHA-256 as a more secure alternative to SHA-1.

# Bibliography

[b-TIA 1050] TIA 1050-100, Project Number 3-0174-000, *Wireless Local Area Network (WLAN) Interworking*.

[b-FIPS 180-2] NIST Federal Information Processing Standards, Publication FIPS 180-2 (2002), *Secure Hash Standard*.

[b-EUROCRYPT] BOYKO (V.), MACKENZIE (P.), PATEL (S.): Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman, EUROCRYPT 2000.

[b-IEEE P1363.2] IEEE P1363.2 (Sept. 2006), *Standard Specifications for Password-Based Public-Key Cryptographic Techniques*.

## 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 |

Printed in Switzerland
Geneva, 2007