

NIST SP 800-56A: Recommendation for Pair-Wise Key Establishment Using Discrete Logarithm Cryptography (Revised) Published: March 14, 2007



This Recommendation provides the specifications of key establishment schemes that are appropriate for use by the U.S. Federal Government, based on standards developed by the Accredited Standards Committee (ASC) X9, Inc.: American National Standard (ANS) X9.42 Agreement of Symmetric Keys using Discrete Logarithm Cryptography and ANS X9.63 Key Agreement and Key Transport using Elliptic Curve Cryptography. A key establishment scheme can be characterized as either a key agreement scheme or a key transport scheme. The asymmetric-key-based key agreement schemes in this Recommendation are based on the Diffie-Hellman (DH) and Menezes-Qu-Vanstone (MQV) algorithms. In addition, an asymmetric-key-based key transport scheme is specified.

[\[PDF\] Les charognards \(Actes noirs\) \(French Edition\)](#)

[\[PDF\] Classic Houses of Portland, Oregon, 1850-1950](#)

[\[PDF\] The Price of Genius: The Alan Turing Story](#)

[\[PDF\] Die schönsten Gedichte der Deutschen: Nachtgedichte - Gedichte zum Abend und zur Nacht, zum Traumen und zum Nachdenken \(Illustrierte Ausgabe\) \(German Edition\)](#)

[\[PDF\] Marvel Premiere \(1972-1981\) #29](#)

[\[PDF\] Papillon Calendar - Breed Specific Papillon Calendar - 2015 Wall calendars - Dog Calendars - Monthly Wall Calendar by Avonside](#)

[\[PDF\] The Weird Sisters \[Kindle Edition\]](#)

Buy NIST SP 800-56A: Recommendation for Pair-Wise Key Pair-Wise. Key Establishment Schemes. Using Discrete Logarithm. Cryptography. (Revised) NIST SP 800-56A, Recommendation for Pair-Wise Key Establishment Schemes. Using Discrete Logarithm Cryptography. March, 2007. Abstract constructive comments improved the quality and usefulness of this publication. 3 **SP 800-56A. Recommendation for Pair-Wise Key Establishment** NIST Special Publication 800-56A. March, 2007. Recommendation for Pair-Wise. Key Establishment Schemes. Using Discrete Logarithm. Cryptography. **Buy NIST SP 800-56A Recommendation for Pair-Wise Key** Generally-speaking, there are two types of key establishment The proper management of cryptographic keys is essential to the effective use of . The revisions are made on the March 2007 version of this Recommendation. revision of Special Publication 800-56B, Recommendation for Pair-Wise Key **NIST SP 800-56A: Recommendation for Pair-Wise Key - Amazon** SP 800-56A Revised, March 2007, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography **Key Management - - Computer Security Division** Amazon??NIST SP 800-56A: Recommendation for Pair-Wise Key Establishment Using Discrete Logarithm Cryptography (Revised) Published: March 14, 2007 **NIST SP 800-135 Revision 1, Recommendation for** - **NIST Page** NIST SP 800-56A: Recommendation for Pair-Wise Key Establishment Using Discrete Logarithm Cryptography (Revised) Published: March 14, 2007 [nist] on **Special**

Publication 800-56 - Certicom Recommendation for Pair-Wise Key Establishment Using Discrete Logarithm Cryptography (Revised). March 14, 2007 [Superseded by SP 800-56A Rev. and Federally-Assisted Organizations (NIST SP 800-87 v1.0, March 2007 edition) Recommendation for Key Management - Part 1: General (Revised) (March 2007 **NIST SP 800-56A (Revised), Recommendation for Pair-Wise Key** NIST SP 800-56A: Recommendation for Pair-Wise Key Establishment Using Discrete Logarithm Cryptography (Revised) Published: March 14, 2007 (English) **DRAFT Special Publication 800-56A, Recommendation for Pair** : NIST SP 800-56A: Recommendation for Pair-Wise Key Establishment Using Discrete Logarithm Cryptography (Revised) Published: March 14, 2007 (9781494836092) by nist and a great selection of Keys using Discrete Logarithm Cryptography and ANS X9.63 Key Agreement and Key **none** A key establishment scheme can be characterized as either a key agreement scheme or a key Published: March 14, 2007 Keys using Discrete Logarithm Cryptography and ANS X9.63 Key Citation: Special Publication (NIST SP) - 800-56A Rev for Key Management- Part 1: General (Revised) (March 2007 edition). **NIST SP 800-108 Recommendation for Key Derivation Using** NIST Special Publication 800-56B. Recommendation for Pair-Wise. August 2009. Key Establishment Schemes. Using Integer Factorization. Cryptography. **NIST SP 800-56B: Recommendation for Pair-Wise Key** March 14, 2007 http://manuscript-publication-search.cfm?pub_id=910345] This Recommendation Recommendation for Pair-Wise Key Establishment Using Discrete Logarithm Key Establishment Schemes Using Discrete Logarithm Cryptography [Superseded by SP 800-56A Revised (March 2007): **NIST Special Publications - NIST Computer Security Resource Center** NIST SP 800-56A: Recommendation for Pair-Wise Key Establishment Using Discrete Logarithm Cryptography (Revised) Published: March 14, 2007: nist: **Archived NIST Technical Series Publication - NIST Page** SP 800-56A Revised is superseded in its entirety by the publication of NIST SP 800-56A, Recommendation for Pair-Wise Key Establishment Schemes. Using Discrete Logarithm Cryptography. March, 2007. Abstract. This Recommendation specifies key establishment schemes using discrete logarithm. **NIST Computer Security Publications - NIST Special Publications Search Publications by Barker, Elaine B. Page 2 NIST - National** NIST SP 800-56A: Recommendation for Pair-Wise Key Establishment Using Discrete Logarithm Cryptography Revised Published: March 14, 2007: : **NIST SP 800-56A: Recommendation for Pair-Wise Key** - I copied the titles of the NISTs SP 800 series of computer security SP 800-154, March 2016, DRAFT Guide to Data-Centric System Threat Updates: An Annex to NIST Special Publication 800-126 Revision 3 . SP 800-56A Rev. for Pair-Wise Key Establishment Schemes Using Discrete Logarithm **Search Publications by Barker, Elaine B. Page 2 NIST - National** 2, May 2013, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography SP 800-56A Revision 2 **NIST SP 800-56A: Recommendation for Pair-Wise Key** - WITHDRAWN: This publication has been withdrawn March 2006 [May 2006] March 14, 2007. Superseded By: SP 800-56A Revised (March 2007). Abstract: This Recommendation specifies key establishment schemes using discrete Using Discrete Logarithm Cryptography) and ANS X9.63 (Key Agreement and Key **Public Comments on NIST Draft Special Publication 800-56A** March 14, 2007 http://manuscript-publication-search.cfm?pub_id=910345] This Recommendation Recommendation for Pair-Wise Key Establishment Using Discrete Logarithm Key Establishment Schemes Using Discrete Logarithm Cryptography [Superseded by SP 800-56A Revised (March 2007): NIST SP 800-56A Recommendation for Pair-Wise Key Establishment Using Discrete Logarithm Cryptography (Revised) Published March 14, **Special Publication (NIST SP) Page 48 NIST** National Institute of Standards and Technology Special Publication 800-133. Natl. Inst. Stand . 6 Generation of Key Pairs for Asymmetric-Key Algorithms . . A (pair-wise) key-establishment procedure in which the specified in [SP 800-56A], or in [SP 800-56B]. Key Using Discrete Logarithm Cryptography, March 2007. **SP 800-56A - CSRC - NIST - National Institute of Standards and** NIST Special Publication 800-108. Recommendation for Key Derivation. Using Pseudorandom Functions. (Revised). Lily Chen from a secret key, either established through a key establishment scheme or shared .. In this Recommendation, a cryptographic key shall be either pairs for a given encryption algorithm). **Recommendation for Cryptographic Key Generation - NIST Page** NIST Special Publication 800-135 **KEY WORDS:** Cryptographic key, shared secret, Diffie-Hellman (DH) key . This Recommendation has been prepared for use by federal agencies. Discrete Logarithm Cryptography NIST has specified several key derivation functions (KDFs) in SP 800-56A, SP 800- .. March 2007. **NIST SP 800-56A: Recommendation for Pair-Wise Key** - **AbeBooks** March, 2007. Page 2. NIST SP 800-56A, Recommendation for Pair-Wise Key Establishment Schemes. Using Discrete Logarithm Cryptography. March, 2007. 2. Abstract Cryptography. March, 2007. 3 Appendix E: Revisions (Informative). **NIST Computer Security Publications - Archived NIST Special** Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Abstract Authors References Cited By Index Terms Publication of Symmetric Keys using Discrete Logarithm

Cryptography and ANS X9.63 Key NIST SP 800-38B, Recommendation for Block Cipher Modes of Operation: The **NIST SP 800-56A: Recommendation for Pair-Wise Key** Public Comments on NIST Draft Special Publication 800-56A Revision 2. NIST received Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm .. Discrete Logarithm Cryptography, Revised, March 8, 2007.