

Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)



This Recommendation specifies key establishment schemes using discrete logarithm cryptography, based on standards developed by the Accredited Standards Committee (ASC) X9, Inc.: ANS X9.42 (Agreement of Symmetric Keys Using Discrete Logarithm Cryptography) and ANS X9.63 (Key Agreement and Key Transport Using Elliptic Curve Cryptography).

Recommendation for Pair-Wise Key Establishment Schemes Using DRAFT Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Draft Revision). **Recommendation for Pair-Wise Key Establishment Schemes Using** on Draft Revision NIST SP 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography **Recommendation for Pair-Wise Key Establishment Schemes Using** Superseded by SP 800-56A Revised (March 2007): specifies key establishment schemes using discrete logarithm cryptography, based on **Recommendation for Pair-Wise Key Establishment - CiteSeerX** Nist Special Publication 800-56a Revision 2: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. **SP 800-56B. Recommendation for Pair-Wise Key Establishment** NIST Special Publication 800-56A. Revision 2. Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. **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 **NIST Special Publications - NIST Computer Security Resource Center** This Recommendation specifies key-establishment schemes based on the discrete logarithm [Supersedes SP 800-56A Revised (March 2007): Diffie-Hellman, elliptic curve cryptography, finite field cryptography, key agreement, key confirmation, key derivation, key establishment, key transport, MQV. **NIST SP 800-108 Recommendation for Key Derivation Using** NIST Special Publication (SP) 800-56B, Revision 1. Title: Wise Key Establishment Schemes Using Integer Factorization Cryptography. SP 800-56B Using Discrete Logarithm Cryptography, Revision 2, May 2013. **NIST SP 800-56B: Recommendation for Pair-Wise Key** Recommendation for Pair-Wise Key Establishment Schemes Using Integer . Key Establishment Schemes Using Discrete Logarithm Cryptography, Revision 1, **Recommendation for Pair-Wise Key Establishment Schemes Using** KEY WORDS: Cryptographic key, shared secret, Diffie-Hellman (DH) key exchange, hash function . Keys Using Discrete Logarithm Cryptography (ANS X9.42-2001) [ANS X9.42] (also in the Financial Services Industry: Key Agreement and Key Transport Using Recommendations for Pair-Wise Key Establishment. **CSRC - Detail** Revision 2. Recommendation for Pair-Wise Key Establishment Schemes Using Discrete. Logarithm Cryptography. Elaine Barker. Lily Chen. Allen Roginsky. **Draft Special Publication 800-56B Rev. 1, Recommendation for Pair** Using Discrete Logarithm Cryptography This Recommendation specifies key establishment schemes using discrete NIST SP 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Appendix E: Revisions (Informative). **NIST SP 800-56A, Recommendation**

for Pair-Wise Key Superseded by SP 800-56A Revised (March 2007): specifies key establishment schemes using discrete logarithm cryptography, based on **Recommendation for Pair-Wise Key Establishment - NIST Page** (SP 800-131A Revision 1) provides more specific guidance for transitions to the use of stronger cryptographic keys and more robust algorithms. [SP 800-56A] NIST Special Publication (SP) 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm **Recommendation for Pair-wise Key Establishment Schemes Using** b) Providing a recommendation for minimum security controls for information systems SP 800-56A specifies key establishment schemes using discrete logarithm for Pair-Wise Key Establishment Using Integer Factorization Cryptography, Recommendation for Key Management Part 1: General (Revised, March 2007, **Recommendation for Pair-Wise Key Establishment Using Discrete** SP 800-175A, August 2016, Guideline for Using Cryptographic Standards . Updates: An Annex to NIST Special Publication 800-126 Revision 3 (Draft), December 2015, DRAFT A Recommendation for the Use of PIV . for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography **Recommendation for Pair-Wise Key Establishment Schemes Using** Livros Nist Special Publication 800-56a Revision 2: Recommendation for Pair-wise Key Establishment Schemes Using Discrete Logarithm Cryptography - U. S. **Framework for Designing Cryptographic Key Management Systems - Google Books Result** A key establishment scheme can be characterized as either a key Keys using Discrete Logarithm Cryptography and ANS X9.63 Key **Public Comments on NIST Draft Special Publication 800-56A** Special Publication 800-56A Revision 2., Recommendation for Pair-Wise Key-Establishment. Schemes Using Discrete Logarithm Cryptography. (May 2013),. [Cfrg] **Fwd: NIST Requests Comments on Draft Revision NIST SP** Annex D: Approved Key Establishment Techniques for FIPS PUB 140-2, . Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Using. Discrete Logarithm Cryptography from Revision 1 to Revision 2. Superseded by SP 800-56A Revised (March 2007): specifies key establishment schemes using discrete logarithm cryptography, based on **Recommendation for Pair-Wise Key Establishment Schemes Using** This Recommendation specifies key establishment schemes using integer **KEY WORDS:** assurances integer factorization cryptography key agreement key NIST SP 800-56B: Recommendation for Pair-Wise Key Establishment Schemes. **KEY ESTABLISHMENT SCHEMES - NIST Page** Recommendation for Pair-Wise Key Establishment Schemes Using Discrete SP 800-56A Revised (March 2007). Abstract: This Recommendation specifies key-establishment schemes based on the discrete logarithm problem over finite fields cryptography finite field cryptography key-agreement key-confirmation key **SP 800-56A. Recommendation for Pair-Wise Key Establishment** Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm. Cryptography, Revision 2 (August 2012). Most comments were **NIST SP 800-56A: Recommendation for Pair-Wise Key Transitions: Recommendation for Transitioning the Use - NIST Page** Superseded by SP 800-56A Revised (March 2007): Recommendation specifies key establishment schemes using discrete logarithm cryptography, based on **DRAFT Special Publication 800-56A, Recommendation for Pair** Buy Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised) on ? **FREE SHIPPING on Recommendation for Pair-Wise Key Establishment Schemes Using** Abstract. This Recommendation specifies key-establishment schemes using integer A (pair-wise) key-establishment procedure where the resultant secret Using Discrete Logarithm Cryptography, Revision 2, May 2013.