1. Record Nr. UNINA9910695198203321

| | |
|---|---|
| Autore | Polk William T |
| Titolo | Cryptographic algorithms and key sizes for personal identity verification [[electronic resource] /] / W. Timothy Polk, Donna F. Dodson, William E. Burr |
| Pubbl/distr/stampa | Gaithersburg, MD : , : U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, , [2005] |
| Edizione | [Draft.] |
| Descrizione fisica | 103 unnumbered pages : digital, PDF file |
| Collana | NIST special publication ; ; 800-78 |
| Altri autori (Persone) | DodsonDonna F<br>BurrWilliam E |
| Soggetti | Computer security - Standards<br>Data encryption (Computer science) |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Note generali | Title from title screen (viewed on May 17, 2005).<br>"April 2005." |
| Nota di bibliografia | Includes bibliographical references. |
| Sommario/riassunto | SP 800-78-1 has been modified to enhance interoperability, simplify the development of relying party applications, and enhance alignment with the National Security Agency's Suite B Cryptography [SUITE B]. Revision 1 reduces the set of elliptic curves approved for use with PIV cards and the supporting infrastructure from six curves to two. Also, SHA-384 has been added for use with Curve P-384 in this revision. And finally, this revision eliminates the largest size of RSA keys (3072 bits) on PIV cards. These changes simplify applications that require maximum interoperability: the number of OIDs that must be recognized (e.g., in certificates) has been significantly reduced; and elliptic curve implementations of elliptic curve cryptography can be optimized for operations over two specific curves. |