

1. Record Nr.	UNINA9910440329203321
Titolo	IEEE Standard Specifications for Password-Based Public-Key Cryptographic Techniques / / Institute of Electrical and Electronics Engineers
Pubbl/distr/stampa	New York : , : IEEE, , 2008
ISBN	0-7381-6016-4
Descrizione fisica	1 online resource (ix, 127 pages)
Disciplina	005.82
Soggetti	Digital signatures Public key cryptography
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Sommario/riassunto	This standard covers specifications of public-key cryptographic techniques for password-based authentication and key establishment, supplemental to the techniques described in IEEE Std 1363-2000 and IEEE Std 1363a-2004. It is intended as a companion standard to IEEE Std 1363-2000 and IEEE Std 1363a-2004. It includes specifications of primitives and schemes designed to utilize passwords and other low-grade secrets as a basis for securing electronic transactions, including schemes for password-authenticated key agreement and password-authenticated key retrieval. Keywords: authentication, key agreement, password, public-key cryptography.