

INTERNATIONAL STANDARDIZED PROFILE

ISO/IEC
ISP
15125-7

First edition
1998-11-15

Information technology — International Standardized Profiles ADYnn — OSI Directory —

Part 7:

ADY43 — DSA to DSA Authentication

*Technologies de l'information — Profils normalisés internationaux
ADYnn — Annuaire OSI —*

Partie 7: ADY43 — Authentification de DSA à DSA



Reference number
ISO/IEC ISP 15125-7:1998(E)

Contents

1 Scope	1
1.1 General	1
1.2 Position within the taxonomy	1
1.3 Scenario	2
2 Normative references	2
2.1 Paired CCITT Recommendations International Standards equivalent in technical content	2
2.2 Normative Amendments and Technical Corrigenda	3
2.3 Additional normative references	4
3 Definitions	4
3.1 General	4
3.2 Support Level	5
4 Abbreviations	5
5 Conformance	6
5.1 Static Conformance Requirements	7
6 Procedures	12
6.1 Introduction	12
6.2 Two-way Authentication	12
6.3 Random Numbers	14
6.4 Distinguished Encoding Rules	14
6.5 Simple Unprotected Authentication	15
6.6 Simple Protected Authentication	16
6.7 Strong Authentication in the DSA, DOP, or DISP Bind	17
6.8 Signed DSP or DISP operations	18
6.9 Merging signed results	20
6.10 Certificates	20
6.11 Access Control Identity in the Distributed Directory	21
6.12 Error Handling	23
Annex A (normative) Profiles Requirements List	26
Annex B (normative) Amendments and Technical Corrigenda	43
Annex C (informative) Commonly Used Algorithms	44