ISO/IEC 17922:2017-09 (E)

Information technology - Security techniques - Telebiometric authentication framework using biometric hardware securit y module

Contents

Page

1 Scope 1
2 Normative references 1
2.1 Identical Recommendations | International Standards 1
2.2 Paired Recommendations | International Standards equivalent in technical content 2
2.3 Additional references 2
3 Definitions 2
3.1 Terms defined in this Recommendation | International Standard 2
3.2 Terms defined in other International Standards 2
4 Abbreviations 3
5 Symbols and terminology 3
6 Biometric hardware security module for telebiometric authentication 3
6.1 Additional feature of BHSM to the HSM 3
6.2 General scenario for use of the BHSM 4
6.3 Telebiometric authentication using the BHSM 4
7 Telebiometric authentication with biometric hardware security module 5
7.1 General 5
7.2 Enrolment procedures 5
7.3 Telebiometric authentication processes 7
8 BHSM based telebiometric authentication procedures 9
8.1 PSID generation and ITU-T X.509 certificate 9
8.2 BHSM based telebiometric authentication process 10
8.3 ASN.1 type for the encrypted PSID 10
Annex A – PSID and related information 11
A.1 General 11
A.2 Encrypted PSID requesting an ITU-T X.509 certificate 11
A.3 ASN.1 for PSID 11
Annex B – Procedures for inserting PSID using PKCS #10 with modification 13
Bibliography 14