ISO/IEC 15045-3-1:2024-12 (E)

Information technology - Home Electronic System (HES) gateway - Part 3-1: Privacy, security, and safety - Introduction

Contents

Page

FOREWORD 4
INTRODUCTION 6
0.1 Overview 6
0.2 Relation to existing work 6
0.3 Relevant affected stakeholder categories 7
1 Scope 9
2 Normative references 9
3 Terms, definitions and abbreviated terms 9
3.1 Terms and definitions 9
3.2 Abbreviated terms 11
4 Conformance 11
5 Protection of privacy, security, and safety 11
5.1 Privacy, security and safety concepts and principles in the HES gateway 11
5.2 Structural protections provided by the HES gateway system 11
5.3 Interface and application services protections 12
5.3.1 Key concepts, principles and practices 12
5.3.2 HES concept 12
5.3.3 HES gateway concept 12
5.3.4 Interface module concept 13
5.3.5 Service module concept 13
5.3.6 Application platform concept 13
5.3.7 Internal communication bus concept 13
5.3.8 DSS principle and practice 13
5.4 Operational protections 14
5.5 Risk management 14
5.5.1 Overview 14
5.5.2 Risk assessment 14
5.5.3 Risk treatment 27
5.6 Privacy, security, and safety guidelines and requirements 28
5.6.1 Privacy-by-design approach 28
5.6.2 External services non-reliance principle and practice 28
5.6.3 Use of wireless or shared media principle and practice 28
5.6.4 Privacy best practice 29
5.6.5 Privacy next best practice 29
5.6.6 Online update vulnerability principle 29
5.6.7 Online OS update vulnerability principle 29
5.6.8 "Social engineering" vulnerability principle 29
5.6.9 Privacy-by-design principle and practice 29
5.6.10 User priority principle 29
5.6.11 Fail-safe principle 30
5.6.12 Precautionary principle 30
5.6.13 Normal accident principle 30

5.6.14 Privacy principles 30
5.6.15 Watchdog practice 30
5.6.16 Redundancy principle 30
6 Common services 30
6.1 Common services 30
6.2 Binding map 31
6.3 HES gateway unique ID service module 31
6.4 Cryptographic services 31
6.5 Authorization and authentication service 31
6.6 Time service 32
Annex A (informative) Privacy protection principles and sources 33
A.1 Privacy protection principles 33
A.2 Sources 33
Annex B (informative) Guidance to developers 35
B.1 General protection 35
B.2 Privacy protection 35
B.3 Security protection 36
B.4 Safety protection 36
Bibliography 38

Figure 1 – ISO/IEC 15045-3-1 within the core interoperability and HES gateway standards 8
Figure 2 – HES gateway generalized architecture 12
Figure 3 – Risk assessment diagram 15
Figure 4 – HAN masquerade and replay 16
Figure 5 – WAN masquerade and replay 17
Figure 6 – HAN interception: eavesdropping and modification 18
Figure 7 – WAN interception: eavesdropping and modification 20
Figure 8 – HAN denial-of-service and resource-exhaustion attack 21
Figure 9 – WAN denial-of-service and resource-exhaustion attack 22
Figure 10 – Worm, virus or Trojan horse 23
Figure 11 – Risk level for HAN: example 26
Figure 12 – Risk level of data inside user objects: example 27
Figure 13 – Risk treatment and risk assessment flow 28
Figure A.1 – Primary sources for privacy protection principles 34