IEC/TR 80001-2-9:2017-08 (E)

Application of risk management for IT-networks incorporating medical devices - Part 2-9: Application guidance - Guidance for use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2 security capabilities

Contents

Page

FOREWORD 4
INTRODUCTION 6
1 Scope 8
2 Normative references 8
3 Terms, definitions and abbreviated terms 9
3.1 Terms and definitions 9
3.2 Abbreviated terms 12
4 ASSURANCE case 12
5 Use of this document 13
5.1 Intended use 13
5.2 Intended audience 13
5.2.1 Intended purpose 13
5.2.2 MEDICAL DEVICE MANUFACTURERS (MDM) 13
5.2.3 Healthcare delivery organizations (HDO) 14
5.2.4 Other stakeholders 15
6 General guidelines 15
6.1 General 15
6.2 Overview of the SECURITY CASE framework 15
6.3 Notation 16
6.3.1 Components of a SECURITY CASE 16
6.3.2 Goal 16
6.3.3 Strategy 17
6.3.4 Justification 17
6.3.5 Context 17
6.3.6 Solution (EVIDENCE) 18
6.3.7 Stakeholder 18
6.3.8 Notation extensions 18
7 Developing the SECURITY CASE 19
8 SECURITY CASE change management 28
Annex A (informative) Exemplar SECURITY PATTERNS 29
A.1 General 29
A.2 Exemplar SECURITY PATTERN for person authentication (PAUT) — SECURITY CAPABILITY PAUT established by MDM for a medical system 29
A.2.1 Goal G6: Replay attack mitigated 29
A.2.2 Goal G8: ‘Man-in-the-middle’ attack mitigated 29
A.2.3 Goal G10: Brute force attack mitigated 29
A.2.4 Goal G13, G14: Denial of service attacks due to account lockout controls mitigated 30

A.3 Exemplar SECURITY PATTERN for automatic logoff (ALOF) established for a thin client terminal system 31
A.3.1 Goal: Patient safety RISK with short session timeouts in OR mitigated 31
A.3.2 Goal: Patient safety RISK with restoring sessions in the OR and ICU mitigated 31
A.4 Exemplar SECURITY PATTERN for audit controls (AUDT) for a system or a device in a HDO facility such as a pharmacy system or an EMR, where multiple people require access to the same data set— Goal G6: Keep a correct audit trail of attending staff in the OR while sessions are kept open 33
Bibliography 35

Figure 1 – Example GOAL (top-level) 17
Figure 2 – Example strategy 17
Figure 3 – Example justification 17
Figure 4 – Example context 18
Figure 5 – Example solution (EVIDENCE) 18
Figure 6 – Example stakeholder 18
Figure 7 – Leading components – Steps 1 through 9 19
Figure 8 – SECURITY CAPABILITY pattern 22
Figure 9 – SECURITY CASE structure 27
Figure A.1 – Exemplar SECURITY PATTERN for PAUT 30
Figure A.2 – Exemplar SECURITY PATTERN for ALOF 32
Figure A.3 – Exemplar SECURITY PATTERN for AUDT 34

Table 1 – Notation extensions 18
Table 2 – SECURITY CASE steps 1 through 9 20
Table 3 – SECURITY CASE steps 10 through 26 23