SEK Teknisk rapport 80001-2-2

Utgiven	Utgåva	Sida	Ansvarig kommitté
2014-02-19	1	1 (1+51)	SEK TK 62

© Copyright SEK. Reproduction in any form without permission is prohibited.

Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls

(IEC Technical Report 80001-2-2:2012)

Denna publikation ingår i en serie med tekniska rapporter som ansluter till standarden SS-EN 80001-1, Riskhantering tillämpad på IT-nätverk som innehåller eller är kopplade till medicintekniska produkter – Del 1: Roller, ansvar och aktiviteter. Den är avsedd att ge en grund för en diskussion och bedömning av de olika aktörernas roller i riskhanteringsprocessen.

För närvarande finns fyra tekniska rapporter i serien. De är:

Part 2-1: Step-by-step risk management of medical IT-networks – Practical applications and examples

Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls

Part 2-3: Guidance for wireless networks

Part 2-4: Application guidance – General implementation guidance for healthcare delivery organizations

ISSN 1651-1417

ICS 11.040.01

Upplysningar om **sakinnehållet** i rapporten lämnas av
SEK Svensk Elstandard.
Postadress: SEK, Box 1284, 164 29 KISTA
Telefon: 08 - 444 14 00. *Telefax*: 08 - 444 14 30
E-post: sek@elstandard.se. *Internet*: www.elstandard.se

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a säkerhet, prestanda, dokumentation, utförande och skötsel av elprodukter, elanläggningar och metoder. Genom att utforma sådana standarder blir säkerhetskraven tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard
Box 1284
164 29 Kista
Tel 08-444 14 00
www.elstandard.se

CONTENTS

INTRODUCTION

IEC 80001-1, which deals with the application of RISK MANAGEMENT to IT-networks incorporating medical devices, provides the roles, responsibilities and activities necessary for RISK MANAGEMENT. This technical report provides additional guidance in how SECURITY CAPABILITIES might be referenced (disclosed and discussed) in both the RISK MANAGEMENT PROCESS and stakeholder communications and agreements.

The informative set of common, high-level SECURITY CAPABILITIES presented here i intended to be the starting point for a security-centric discussion between vendor and purchaser or among a larger group of stakeholders involved in a MEDICAL DEVICE IT-NETWORK project. Scalability is possible across a range of different sized RESPONSIBLE ORGANIZATIONS as each evaluates RISK under the capabilities and decides what to include or not include according to its RISK tolerance and resource planning. This technical report might be used in the preparation of documentation designed to communicate product SECURITY CAPABILITIES and options. This documentation could be used by the RESPONSIBLE ORGANIZATION as input to their IEC 80001 PROCESS or to form the basis of RESPONSIBILITY AGREEMENTS among stakeholders. Other IEC-80001-1 technical reports will provide step-by-step guidance in the RISK MANAGEMENT PROCESS. Furthermore, the SECURITY CAPABILITIES encourage the disclosure of more detailed security controls – perhaps those specified in one or more security standards as followed by the RESPONSIBLE ORGANIZATION or the MEDICAL-DEVICE manufacturer (for example, ISO 27799:2008, ISO/IEC 27001:2005, ISO/IEC 27002:2005, ISO/IEC 27005:2011, the ISO 22600 series, the ISO 13606 series, and ISO/HL7 10781:2009, which covers the Electronic Health Record System Functional Model). This report remains agnostic as to the underlying controls framework; it only proposes a structure for the disclosure and communication among the RESPONSIBLE ORGANIZATION (here called the healthcare delivery organization – HDO), the MEDICAL DEVICE manufacturer (MDM) and the IT-vendor.

The capabilities outlined here comprise a disclosure set of controls which support the maintenance of confidentiality and the protection from malicious intrusion that might lead to compromises in integrity or system/data availability. Capabilities can be added to or further elaborated as the need arises. Controls are intended to protect both data and systems but special attention is given to the protection of both PRIVATE DATA and its subset called HEALTH DATA. Both of these special terms have been defined to carefully avoid any law-specific references (e.g., EC Sensitive Data or USA ePHI).

APPLICATION OF RISK MANAGEMENT FOR IT-NETWORKS INCORPORATING MEDICAL DEVICES –

Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls

1 Scope

This part of IEC 80001 creates a framework for the disclosure of security-related capabilities and RISKS necessary for managing the RISK in connecting MEDICAL DEVICES to IT-NETWORKS and for the security dialog that surrounds the IEC 80001-1 RISK MANAGEMENT of IT-NETWORK connection. This security report presents an informative set of common, high-level security-related capabilities useful in understanding the user needs, the type of security controls to be considered and the RISKS that lead to the controls. INTENDED USE and local factors determine which exact capabilities will be useful in the dialog about RISK.

The capability descriptions in this report are intended to supply:

a) health delivery organizations (HDOs),

b) MEDICAL DEVICE manufacturers (MDMs), and

c) IT vendors

with a basis for discussing RISK and their respective roles and responsibilities toward its management. This discussion among the RISK partners serves as the basis for one or more RESPONSIBILITY AGREEMENTS as specified in IEC 80001-1.

The present report provides broad descriptions of the security-related capabilities with the intent that any particular device or use of a device will have to have at least one additional level of specification detail under each capability. This will often be site and application-specific and may invoke RISK and security controls standards as applicable.

At this introductory stage of IEC 80001-1 standardization, the SECURITY CAPABILITIES in this report provide a common, simple classification of security controls particularly suited to MEDICAL IT NETWORKS and the incorporated devices. The list is not intended to constitute or to support rigorous IT security standards-based controls and associated programs of certification and assurance such as might be found in other ISO standards (e.g., ISO/IEC 15408 with its Common Criteria for Information Technology Security Evaluation). The present report does not contain sufficient detail for exact specification of requirements in a request for proposal or product security disclosure sheet. However, the classification and structure can be used to organize such requirements with underlying detail sufficient for communication during the purchase and integration PROCESS for a MEDICAL DEVICE or IT equipment component. Again, this report is intended to act as a basis for discussion and agreement sufficient to initial integration project RISK MANAGEMENT. Additionally, security only exists in the context of the organizational security policies. Both:

a) the security policies of the healthcare delivery organization (HDO), and

b) the product and services security policies of the MEDICAL DEVICE manufacturer (MDM)

are outside of the scope of this report. In addition, the Technical Report does not address clinical studies where there is a need for securing the selective disclosure of PRIVATE DATA or HEALTH DATA.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 80001-1:2010, *Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities*