ISO/IEC TS 19608:2018 (E)

Guidance for developing security and privacy functional requirements based on ISO/IEC 15408

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Symbols and abbreviated terms

5 Purpose and structure of this document

6 Requirement definition

6.1 General
6.2 Security functional requirements (SFRs)
6.2.1 General
6.2.2 Example of security functional requirements
6.2.3 The selection, assignment, refinement and iteration operations
6.2.4 Dependencies between components
6.2.5 Structure of security functional components
6.2.6 List of classes
6.3 Procedure to specify security functional requirements
6.4 Procedure to develop functional components
6.4.1 Procedure
6.4.2 Existing components for privacy requirements in ISO/IEC 15408-2
6.4.3 Extended components for privacy requirements in published PP/STs and research papers

7 Privacy principles

7.1 General
7.2 Input for extended components
7.3 Procedure to develop privacy requirements from privacy principles
7.4 Extended components for privacy
7.4.1 “Consent and choice” principle
7.4.1.1 General
7.4.1.2 Presenting choice and obtaining consent
7.4.1.3 Reaffirming the choice selected
7.4.1.4 Preserving a record of choices
7.4.1.5 Exempting PII from processing upon modification or withdrawal of consent
7.4.2 "Purpose legitimacy and specification" principle
7.4.3 "Collection limitation" principle: Collecting PII
7.4.4 "Data minimization" and "Use, retention and disclosure limitation" principles
7.4.4.1 Minimizing PII
7.4.4.1.1 General
7.4.4.1.2 Minimize PII by filtering and removal
7.4.4.1.3 Minimize sensitivity of PII by conversion
7.4.4.1.4 Minimize identifiability of PII by use of anonymity, pseudonymity, unlinkability and unobservability
7.4.4.1.5 Minimize accumulation of PII by division
7.4.4.1.6 Minimize access to PII
7.4.4.1.7 Minimize PII retention

7.4.5 "Openness, transparency and notice" principle
7.4.6 "Individual participation and access" principle
7.4.6.1 Accessing and reviewing the PII principal's own PII
7.4.7 "Accuracy and quality" principle
7.4.7.1 Changing PII properly
7.4.7.2 Updating PII periodically
7.4.8 "Accountability" and "Privacy compliance" principles
7.4.9 "Information Security" principle
7.4.9.1 Protecting PII

8 Summary of extended components and related privacy principles

8.1 General
8.2 Extended components - general definition
8.2.1 General
8.2.2 "Consent and choice" principle
8.2.2.1 Presenting choice and obtaining consent
8.2.2.2 Reaffirming the choice selected
8.2.2.3 Exempting PII from processing upon modification or withdrawal of consent
8.2.3 "Data minimization" and "Use, retention and disclosure limitation" principles
8.2.3.1 Minimizing PII
8.2.3.1.1 Minimization by filtering and removal
8.2.3.1.2 Minimization sensitivity by conversion
8.2.3.1.3 Minimize retention
8.2.4 "Openness, transparency and notice" principle
8.2.5 "Individual participation and access" principle: Challenging the accuracy and completeness of PII
8.2.6 "Accuracy and quality" principle: Updating PII periodically

Annex A (informative) Existing components used for privacy requirements

A.1 Overview
A.1.1 General
A.1.2 Class FAU: Security Audit
A.1.2.1 General
A.1.2.2 Rationale for the operations made:
A.1.2.3 Class FCO: Communication
A.1.3 Class FCS: Cryptographic support
A.1.4 Class FDP: User data protection
A.1.5 Class FIA: Identification and authentication
A.1.6 Class FMT: Security Management
A.1.7 Class FPR: Privacy
A.1.8 Class FPT: Protection of the TSF
A.1.9 Class FRU: Resource utilization
A.1.10 Class FTA: TOE access
A.1.11 Class FTP: Trusted path/channels
A.2 Protection Profile for "Machine-Readable Travel Document with "ICAO Application", Basic Access Control"[2]
A.2.1 TOE
A.2.2 Privacy threat
A.2.3 Functional components

Annex B (informative) Extended components for privacy in existing Protection Profiles

B.1 General
B.2 Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)[3]
B.2.1 TOE
B.2.2 Privacy threat
B.2.3 Extended components
B.3 User-Oriented Protection Profile for Unobservable Message Delivery using MIX networks [4]
B.3.1 TOE
B.3.2 Privacy threats
B.3.3 Extended components
B.3.3.1 General
B.3.3.2 Information retention control (FDP_IRC)

B.3.3.3 Unlinkability (FPR_UNL)
B.3.3.4 Distribution of trust (FPR_TRD)

Annex C (normative) Example of extended components for privacy

C.1 General
C.2 Class FPFW: Privacy Requirements from the ISO/IEC 29100 Privacy Framework
C.2.1 General
C.2.2 Choice
C.2.2.1 Family behaviour
C.2.2.2 Component levelling
C.2.2.3 FPFW_COI.1 Presentation of choice
C.2.3 Obtaining consent
C.2.3.1 Family behaviour
C.2.3.2 Component levelling
C.2.3.3 FPFW_CON.1 Obtaining consent
C.2.4 Notification of choice
C.2.4.1 Family behaviour
C.2.4.2 Component levelling
C.2.4.3 FPFW_NOC.1 Reaffirmation of choice
C.2.5 Modification of choice or consent
C.2.5.1 Family behaviour
C.2.5.2 Component levelling
C.2.5.3 FPFW_MOC.1 Modification of choice
C.2.6 Removal of PII
C.2.6.1 Family behaviour
C.2.6.2 Component levelling
C.2.6.3 FPFW_RMV.1 Filtering and removal
C.2.7 Conversion of PII
C.2.7.1 Family behaviour
C.2.7.2 Component levelling
C.2.7.3 FPFW_CNV.1 Conversion for minimization of sensitivity
C.2.8 Deletion of PII
C.2.8.1 Family behaviour
C.2.8.2 Component levelling
C.2.8.3 FPFW_DEL.1 Deletion or archiving
C.2.9 Information about the PII policy
C.2.9.1 Family behaviour
C.2.9.2 Component levelling
C.2.9.3 FPFW_IPO.1 Access to policy
C.2.9.4 FPFW_IPO.2 Notification of policy changes
C.2.9.5 FPFW_IPO.3 Notification of PII related issues
C.2.10 Review and change of PII
C.2.10.1 Family behaviour
C.2.10.2 Component levelling
C.2.10.3 FPFW_RAC.1 Challenge and correction of PII
C.2.11 Period update
C.2.11.1 Family behaviour
C.2.11.2 Component levelling
C.2.11.3 FPFW_PUD.1 Periodic update time interval
C.2.11.4 FPFW_PUD.2 Informing about periodic update

Page count: 48