DIN EN 16571:2014-10 (E)

Information technology - RFID privacy impact assessment process

Contents

Page

Foreword 5

Introduction 6

1 Scope 7

2 Normative references 7

3 Terms and definitions 7

4 Symbols and abbreviations 11

5 Structure of this European Standard 12

6 Field of reference for this European Standard 12
6.1 'RFID' as defined by the EU RFID Recommendation 12
6.2 'RFID application' as defined by the EU RFID Recommendation 13
6.3 'RFID operator' as defined by the EU RFID Recommendation 13
6.4 Relationship between the RFID PIA and data protection and security 14
6.5 Relevant inputs for the PIA process 17
6.5.1 General 17
6.5.2 The privacy capability statement 17
6.5.3 The Registration Authority 17
6.5.4 RFID PIA templates 17

7 RFID operator's organizational objectives of the RFID PIA 17
7.1 Overview 17
7.2 Meeting and exceeding legal requirements 18
7.3 When to undertake the RFID PIA 19
7.3.1 General 19
7.3.2 Undertaking a PIA at the design stage before the RFID system becomes operational 19
7.3.3 Undertaking a PIA at a review and update the design-based PIA 19
7.3.4 Undertaking a PIA to contribute to the development of a template 19
7.3.5 Undertaking a PIA with an established template 20
7.3.6 Undertaking a PIA at the introduction of a new function within the RFID application 20
7.3.7 Undertaking a PIA based on changes in RFID technology 20
7.3.8 Undertaking a PIA when a privacy breach has been reported 20

8 Tools to simplify the process 21
8.1 RFID operator responsibility 21
8.2 RFID technology privacy capability tools - overview 21
8.3 Registration of RFID privacy capability statements by RFID product manufacturers 21
8.3.1 General 21
8.3.2 Obligations of the Registration Authority 21
8.3.3 Appointment 22
8.3.4 Resignation 22
8.3.5 Responsibilities of the RFID product manufacturers 22
8.4 RFID technology privacy capability tools - details 23
8.4.1 RFID integrated circuit privacy capabilities 23
8.4.2 RFID tag privacy capabilities 23
8.4.3 RFID interrogator privacy capabilities 23
8.4.4 The default privacy capability statement 23

8.4.5 Using CEN/TR 16672 to construct privacy capabilities for products using proprietary protocols ... 24
8.5 Templates ... 24
8.5.1 General ... 24
8.5.2 Developing a template ... 24
8.5.3 Who should prepare the templates? ... 25
8.5.4 The role of stakeholders in template development ... 25

9 RFID PIA - a process approach ... 26
9.1 Introduction ... 26
9.2 Process Steps ... 26
9.3 Achieving the correct level of detail ... 27
9.3.1 General ... 27
9.3.2 Level 0 - no PIA ... 27
9.3.3 Level 1 - small scale PIA ... 27
9.3.4 Level 2 - PIA focussed on the controlled domain of the application ... 27
9.3.5 Level 3 - Full scale (complete) PIA of the application ... 28
9.3.6 Reducing the effort for the SME organization ... 28
9.4 Process methodology ... 29

10 Preparing the RFID functional statement ... 30

11 Preparing the description of the RFID applications ... 31
11.1 Introduction ... 31
11.2 Multiple applications ... 31
11.3 RFID application overview ... 32
11.3.1 General ... 32
11.3.2 Determine which RFID technology is intended or being used ... 32
11.3.3 Determine the RFID components used in the application ... 33
11.3.4 RFID applications on portable devices ... 34
11.4 Data on the RFID tag ... 36
11.4.1 General ... 36
11.4.2 Determine what inherent identifiable features are possessed by the RFID tag ... 36
11.4.3 Listing the data elements encoded on the RFID tag ... 37
11.4.4 Determine whether encoded data can be considered identifiable ... 37
11.4.5 Determine whether personal data is encoded on the tag ... 38
11.5 Additional data on the application ... 38
11.6 RFID data processing ... 38
11.7 Internal transfer of RFID data ... 39
11.8 External transfer of RFID data ... 39
11.9 RFID application description sign off ... 39

12 Risk Assessment ... 40
12.1 Procedural requirements derived from the RFID Recommendation ... 40
12.1.1 Common procedure requirements for all RFID operators ... 40
12.1.2 Requirements for retailers that are RFID operators ... 41
12.1.3 Procedure requirements for manufacturers of products eventually sold to consumers ... 42
12.2 Asset identification and valuation ... 42
12.2.1 General ... 42
12.2.2 Identification of assets ... 43
12.2.3 Valuing assets ... 44
12.3 Threat identification and evaluation ... 47
12.3.1 General ... 47
12.3.2 Identification and classification of threats ... 48
12.3.3 Evaluating threats ... 49
12.3.4 The process for the SME organization ... 50
12.4 Identifying vulnerabilities and enumerating the associated risk levels ... 50
12.4.1 Basic procedure ... 50
12.4.2 Procedure to account for exposure time ... 51
12.5 Initial risk level ... 51
12.6 Countermeasures ... 53
12.6.1 General ... 53

12.6.2 Identifying countermeasures 53
12.6.3 Reassessing risk levels 55
12.7 Residual risks 55
12.8 RFID PIA endorsement 56

13 Worked example of the risk assessment process 56

14 The PIA summary report 56
14.1 PIA report date 56
14.2 RFID application operator 56
14.3 RFID application overview 56
14.4 Data on the RFID tag 56
14.5 RFID Privacy Impact Assessment score 57
14.6 RFID countermeasures 57

15 Revision control 57

16 Monitoring and incident response 58

Annex A (normative) Details of Registration Authority 59

Annex B (informative) RFID manufacturer's product privacy capability statements 60

B.1 RFID integrated circuit (chip) privacy features 60
B.2 RFID interrogator privacy features 62

Annex C (informative) RFID Privacy Impact Assessment flowchart 65

Annex D (informative) Template development 67

Annex E (informative) Flowchart to determine the RFID PIA level 68

Annex F (informative) RFID functional statement 69

Annex G (normative) RFID application description 70

Annex H (informative) Identification and valuation of personal privacy assets 71

H.1 Individually held personal privacy asset 71
H.2 Assets that apply to the organization 76

Annex I (informative) RFID threats 77

I.1 Threats associated with the data encoded on the RFID tag and the RFID tag (or RF card) itself 77
I.2 Threats associated with the air interface or the device interface communication 80
I.3 Threats associated with the interrogator (or reader) 85
I.4 Threats associated with the host application 85

Annex J (informative) Countermeasures 88

J.1 List of countermeasures 88
J.2 Threat and countermeasure mappings 90

Annex K (informative) PIA risk assessment example 94

K.1 Introduction 94
K.2 Ranking the assets 94
K.3 Considering threats at the tag layer and air interface layer 95
K.4 Considering threats at the interrogator layer 96
K.5 Considering threats at the device interface layer 97
K.6 Considering threats at the application layer 97

K.7 Considering vulnerabilities 98
K.8 Risk scores after considering all the threats and vulnerabilities 98
K.9 Applying countermeasures 99
K.10 Overall risk 99

Annex L (informative) RFID Privacy Impact Assessment summary 101

Bibliography 102