RFID Privacy Protection

- Broad Overview of the EU position
- RFID Privacy-centric
- Focus on two critical standards
- Some tools
- Implications for RFID operators
- Timetable
The European Perspective

The key milestones:

• EC Recommendation on RFID privacy and security May 2009
• Mandate M436 Phase 1 on RFID privacy Feb 2010 to Mar 2011: Evaluation of gaps in terms of standardization: TR 187020 v0.0.12
• Mandate M436 Phase 2 assigned to CEN TC225 Apr 1st 2011: Development of 10 necessary standards (*) including 2 fundamental ENs: - 16570 Signage policy and Emblem
  - 16571 Privacy Impact Assessment
• The proposed Data Protection and Privacy Regulation

(*) Covers item management AND contactless applications
The Data Protection and Privacy Regulation

The European Commission plans to unify data protection within the European Union (EU) with a single law, the **General Data Protection Regulation (GDPR)**. The current EU Data Protection Directive 95/46/EC does not consider important aspects like globalization and technological developments like social networks and cloud computing sufficiently and determined that new guidelines for data protection and privacy were required. Therefore a proposal for the regulation has been released on 25 January 2012. In the meantime amendments have been made. The adoption is aimed for in 2014 and the regulation is planned to take effect in 2016 after a transition period of 2 years.
The proposed new EU data protection regime extends the scope of the EU data protection law to all foreign companies processing data of EU residents. It provides for a harmonization of the data protection regulations throughout the EU, thereby making it easier for non-European companies to comply with these regulations; however, this comes at the cost of a strict data protection compliance regime with severe penalties of up to 2% of worldwide turnover.
Privacy, Data Protection, Security and RFID

• **Data Protection:** legal requirement to ensure appropriate collection, consent, retention, correction and use of data collected by an organization from their consumers & users

• **Data Security:** good practice to protect the organization’s data including the data about individuals as well as other operational data held by the organization

• **RFID Privacy:** good practice to ensure that a person carrying an RFID tag or card has his / her privacy protected wherever it is possible to read the tag

Note 1: Privacy focuses on the individual not the corporation

Note 2: Privacy extends beyond the operational domain of the application
RFID Privacy: The individual’s Privacy at the centre

• RFID operator’s responsibilities
  -) Notification & Signage
  -) RFID privacy impact assessment, including risk assessment
  -) Registration (some countries)

• RFID vendor’s responsibilities
  -) technical support on functionalities
  -) contribution to the PIA process

• Product supplier’s responsibilities
  -) RFID privacy impact assessment, including risk assessment
EN 16570
RFID Notification Sign

1: Emblem

2: Purpose of the application
RFID Tags may be read in this area for the purposes of stock control security and product warranty.

This system is controlled by Van Rees B.V.

For more information. Contact us on:
Freephone 0800 800 8888
Or visit our website
www.vanrees.com/privacy
EN 16570
RFID Notification Emblem

From: EN 16656 - ISO/IEC 29160
The European Emblem

• Will co-exist with existing logos:
  – global systems such as contactless payment cards
  – national and local cards. e.g. travel cards
EN 16571  
The Key Privacy Question

- Is an RFID tag carried by or associated with an individual?
- If so, then the asset / data types need to be considered to determine the level of the PIA
  - personally identifiable data or personal behaviour data on the tag does require the strictest Level 3 assessment
  - such data not on the tag, but on the RFID application does require a Level 2 assessment
  - an RFID tag carried or associated with an individual only requires a Level 1 assessment
EN 16571
The PIA Process

Risk = f(Asset, Threat, Vulnerability)
EN 16571
Countermeasures to reduce risks

- 48 countermeasures identified from associated Technical Reports and research within the scope
  - ex retail: deactivation at P.O.S. (kill function)
  - ex bank cards: shielded cases
- Relate to specific threats
- Relate to protocols and products with possible tools to address product features ex: untraceable tags
- Some countermeasures address multiple threats
- Some threats have no countermeasures
EN 16571

Tools

• **Devices privacy capability statements** provided by vendors and on a publicly accessible database (through Registration Authority)

• **Application Templates**, examples:
  – Libraries based on ISO 28560-2
  – Contactless payment cards
  – Staff ID cards

• **Work has begun…**
Implications for RFID Operators

• No legal requirement – yet, but the new Data Protection and Privacy Regulation is on the way.
• The UK DPA is developing legal guidelines for privacy
• There will be pressure to display the sign
• The sign without a summary PIA will expose libraries
• Conclusion: need to move forward in parallel to the standard
• The technology is not without vulnerabilities

➔ .......Enhance privacy and security features.
Privacy by design.
Delivables on Public Awareness

- **FprEN 16656**  
  Radio Frequency identification – RFID Emblem  
  Sent to UAP vote. Ballot closes on 2014-04-07

- **FprEN 16570**  
  Information Technology – Notification of RFID – The Information Sign and additional Information to be provided by operators  
  Sent to Formal vote in February 2014

- **FprCEN/TR 16684**  
  Notification of RFID – Additional Information to be provided by operators  
  Sent to Formal vote. Ballot closes on 2014-02-19

- **FprCEN/TS 16685**  
  Notification of RFID – The Information Sign to be displayed in areas where RFID interrogators are deployed  
  Sent to Formal vote. Ballot closes on 2014-02-19
Delivables on Privacy Impact Assessment (PIA)

- **FprEN 16571**  
  RFID Privacy Impact Assessment Process  
  Sent to Formal vote in February 2014

- **FprCEN/TR 16674**  
  Information Technology – Analysis of PIA methodologies relevant to RFID  
  Sent to Formal vote. Ballot closes on 2013-12-19

- **FprEN/TR 16673**  
  RFID Privacy Impact Assessment analysis for specific sectors  
  Sent to Formal vote. Ballot closes on 2013-12-19
Deliverables on Technical matters

- **FprCEN/TR 16670**  RFID Threat and Vulnerability Analysis
  Sent to Formal vote. Ballot closes on 2013-12-19
- **FprCEN/TR 16672**  Privacy capability features of current RFID technologies
  Sent to Formal vote. Ballot closes on 2013-12-19
- **FprCEN/TR 16671**  Authorization of Mobile Phones when used as RFID Interrogators
  Sent to Formal vote. Ballot closes on 2013-12-19
- **FprCEN/TR 16669**  Device interface to support ISO/IEC 18000-3 standard
  Sent to Formal vote. Ballot closes on 2013-12-19
# Activities | Latest Std | Due date
--- | --- | ---
1 Signature of contract between CEN and the EC | T0 | 2011-12
8 TC review | T+11 | 2012-11
9 Closure of TC review | T+13 | 2013-01
10 Final discussion by TC225 plenary in Brussels | T+13 | 2013-01
11 Submission of interim report to EC | T+14 | 2013-02
12 Submission of final drafts to TC secretary | T+18 | 2013-06
13 Dispatch of final drafts to CCMC for Formal Vote | T+18 | 2013-06
14 Submission to Formal Vote | T+21 | 2013-11
15 Closure of latest Formal Vote | T+24 | 2014-02
16 Definitive texts TSs and TR available | T+25 | 2014-03
17 Publication TSs and TR by CEN | T+28 | 2014-05
18 Submission of final report to EC | T+28 | 2014-06
# M/436 time schedule: ENs

<table>
<thead>
<tr>
<th>#</th>
<th>Activities</th>
<th>Latest Std</th>
<th>due date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Signature of contract between CEN and the EC</td>
<td>T0</td>
<td>2011-12</td>
</tr>
<tr>
<td>10</td>
<td>Submission of Enquiry drafts to TC secretary</td>
<td>T+12</td>
<td>2012-12</td>
</tr>
<tr>
<td>11</td>
<td>Despatch of final drafts to CCMC for Enquiry</td>
<td>T+12</td>
<td>2012-12</td>
</tr>
<tr>
<td>12</td>
<td>Submission of interim report to EC</td>
<td>T+14</td>
<td>2013-02</td>
</tr>
<tr>
<td>13</td>
<td>Submission to Enquiry</td>
<td>T+15</td>
<td>2013-03</td>
</tr>
<tr>
<td>14</td>
<td>Closure of Enquiry</td>
<td>T+19</td>
<td>2013-08</td>
</tr>
<tr>
<td>15</td>
<td>Submission of final drafts to TC secretary</td>
<td>T+21</td>
<td>2013-11</td>
</tr>
<tr>
<td>16</td>
<td>Dispatch of final drafts to CCMC for Formal vote</td>
<td>T+21</td>
<td>2013-11</td>
</tr>
<tr>
<td>17</td>
<td><strong>Submission to Formal vote</strong></td>
<td><strong>T+24</strong></td>
<td><strong>2014-02</strong></td>
</tr>
<tr>
<td>18</td>
<td>Closure of formal vote</td>
<td>T+26</td>
<td>2014-04</td>
</tr>
<tr>
<td>19</td>
<td>Final text available</td>
<td>T+28</td>
<td>2014-05</td>
</tr>
<tr>
<td>20</td>
<td>Submission of Final report to EC</td>
<td>T+28</td>
<td>2014-06</td>
</tr>
<tr>
<td>21</td>
<td>Publication Ens</td>
<td>T+29</td>
<td>2014-07</td>
</tr>
</tbody>
</table>
Thanks for Your Attention

Gérard DESSENNE

more info at: gad13@orange.fr