CONVERGENT SOFTWARE

RFID PRIVACY IN EUROPE
Implications for Libraries

Paul Chartier
Convergent Software Ltd

CILIP Conference, Nov 2012
ISO TC46/SC4/WG11 N246

Today's Presentation

CONVERGENT SOFTWARE

- Broad Overview of the EU position
- A bit of jargon-busting
- CEN TC 225 work on Mandate M 436
- Focus on two critical standards
- Some tools
- Implications for libraries
- Timetable

Déjà Vu

- This is what I presented at last year's Conference

  2011-10-28: European Commission receives a detailed response for standards on RFID privacy
  - All libraries will be expected to undertake a privacy impact assessment, and more
  - New standard interface to support migration to next generation RFID

- This is what I said at last year's Conference

  "There will be a number of European standards and related documents on RFID privacy. Few vendors and few libraries contributed to the public consultation - now it will be a **reality**"

The European Commission

What do you know about:

- Data Protection Directive 95/46/EC?
- EC Recommendation on RFID privacy and security 2009?
- Mandate M436 Phase 1 on RFID privacy?
- And the library sector response to public consultation?
- The proposed Data Protection and Privacy Regulation?
- **Mandate M436 Phase 2 assigned to CEN TC225 ?**

Jargon-busting

- EU legal documents: Recommendations, Directives, Regulations
- European Standards: EN = Standard, TS =Technical Specification, TR = Technical Report
- RFID ~ the EU might have a different view from you
- EU Mandate
- Privacy is different from Data Protection
- RFID application and RFID operator
- Privacy Impact Assessment

CEN TC 225 work on Mandate M 436 – Project Structure

PTA	• Signage and Emblem
PTB	• RFID Device Privacy
PTC	• Privacy Impact Assessment
PTD	• RFID Penetration testing
PTE	• Extended RFID device security capability

CEN TC 225 work on Mandate M 436 – Projects of PT-B, D and E

- **PT-B - TR:** Privacy capability features of current RFID technologies
- **PT-D - TR:** RFID threat and vulnerability analysis
- **PT-E - TR:** Authorisation of mobile phones used as RFID interrogators
- **PT-E - TR:** Device interface to support ISO/IEC 18000-3 Mode 1 and Mode 3 tags

M 436 – Projects of PT-A Signage and Emblem

- TR: Additional information to the signage to be provided by operators
- TS: Information sign to be displayed in areas where RFID interrogators are deployed
- EN: Information sign and additional information to be provided by operators of RFID data capture applications
- The TS and the EN will be released at the same time for review by standards bodies. The EN also undergoes a round of “public review” before publication. At this point the TS will be withdrawn.

RFID Notification Emblem

CONVERGENT SOFTWARE

The European Emblem

CONVERGENT SOFTWARE

- **Current unresolved issue:**
  - coexistence of the Common European Emblem and current logos,
  - especially global systems such as contactless bank cards
  - National and local cards. e.g. travel cards

RFID Notification Sign: Reading Zone

CONVERGENT SOFTWARE

M 436 – Projects of PT-A Privacy Impact Assessment

CONVERGENT SOFTWARE

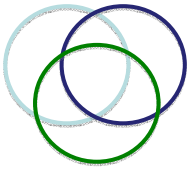
- TR: RFID PIA analysis for specific sectors (retail, libraries, banking, transportation)
- TR: Analysis of PIA methodologies relevant to RFID
- EN: RFID PIA process

- The Technical Reports are intended to set the scene and enable comments to be made to modify the Standard, which has an additional round of review

Privacy, Data Protection, Security and RFID

- **Data Protection:** ensures appropriate collection, consent, correction and use of data collected by an organisation from their consumers & users
- **Data Security**: protects all the organisation's data including the data about individuals as well as other operational data held by the organisation
- **Privacy :** provides an individual's control over the use of collected data by organisations and protection from unauthorised collection of data from ICT in the individual's possession

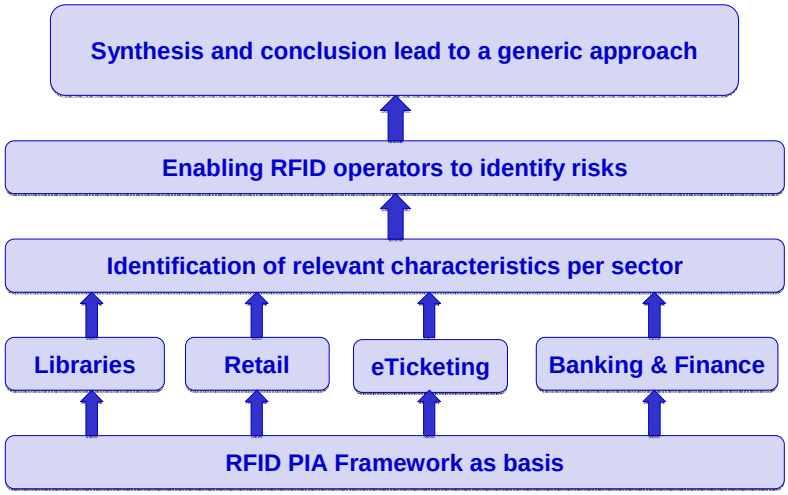
Data Protection, Security and Privacy



Privacy focuses on the individual not the corporation

Privacy extends beyond the operational domain of the application

TR: RFID PIA Analysis for Specific Sectors



EN: RFID Privacy Impact Assessment (PIA) process

CONVERGENT SOFTWARE

Key points from Scope

- It provides a **standardised set of procedures for developing PIA templates**, including tools compatible with the RFID PIA methodology.
- In addition, **it identifies the conditions that require an existing PIA to be revised, amended, or replaced by a new assessment process.**

EN: PIA Process Focus on Privacy

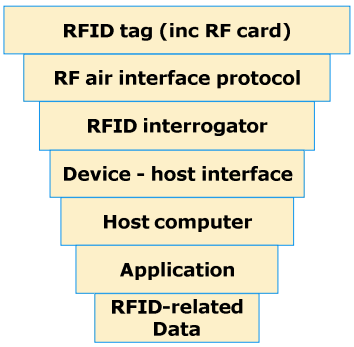
CONVERGENT SOFTWARE

Challenge

- Data is already subject to Data Protection Directive 95/46/EC
- The EN needs to address RFID features and privacy

Approach

- The figure (*based on ISO 27033-2*) shows the complete RFID layered stack
- Each layer needs to be addressed
- Top 4 layers are generally not well-understood from a privacy perspective
- Many optional features in the standards
- The interrogator and tag can differ
- Device to host - **a real challenge with mobile devices like smart phones**



Smartphone: Operational Blessing Privacy Curse?

CONVERGENT SOFTWARE

EN: PIA Process What is Identifiable?

CONVERGENT SOFTWARE

Challenge

- No ambiguity in the Data Protection Directive:
  - Sensitive personal data - name, national ID code, medical records
  - Personal data - membership code
  - Identifiable data - unique chip ID, product code

Approach

- Asset value (asset can be personal privacy)
- Assess threats
- Vulnerabilities (exposure) of assets
- Identify risks = function {asset, threat, vulnerability}
- Controls and mitigations
- Resulting in **residual risk**

Issue: Quantitative or not?

EN: PIA Process Take-up

Challenge

- Both the Recommendation and the EN that we are drafting have no legal basis for implementation

Approach

- The EN will identify, as a best practice, why a PIA needs to be undertaken even for an established RFID system. Here are three drivers:
  - governments (at all levels) as RFID operators: ID cards, transport systems, libraries, even contactless payments. Potentially the best opportunity for rapid take-up
  - to align with sector templates; do organisations want to be exposed as not interested in privacy?
  - the signage, which will have a blank entry for the source of the PIA summary

EN: PIA Process Tools

- EN will describe process and to assist risk assessment list:
  - Assets and associated data elements
  - RFID threats
  - RFID vulnerabilities
- Device privacy capability statements provided by vendors and on a publicly accessible database
- Templates:
  - Sector level e.g. Libraries based on ISO 28560-2
  - Application level e.g. Contactless payment cards, staff id cards

Implications for Libraries

- No legal requirement – **yet, but the new Data Protection and Privacy Regulation is on the way.**
- 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; library ownership might be a factor to accelerate
- The technology is not without vulnerabilities, and more are exposed in the security area
- **Enhancing privacy and security** – ideal driver
- **Who takes the lead in the library sector?**

Timetable for the ENs

- Work started March 2012
- CEN TC 225 meetings in December and January
- Translation
- March 2013 – 5 month public enquiry
- August / September 2013: Final text

- **At this point all technical details are content is stable**
- Translation
- December 2013 – 2-month formal vote, simple Yes/ No
- Publication > February 2014
- **What will the library community have achieved?**


CONVERGENT
SOFTWARE
Thanks for Your Attention
www.convergent-software.co.uk