Privacy-Preserving Management of Personal Data For Assisted-Living Applications

Gina Kounga, Marco Casassa Mont, Pete Bramhall
Researcher

29 November 2010

Outline

- Context
- Problem statement
- Scenario
- Solution
- Conclusion

Context

EnCoRe Project www.encore-project.info

- Aims at allowing data subjects to grant consent to the use of their personal data and to revoke that consent if required
- Existing solutions to manage consent provide data subjects with only limited control over their personal data
- The notion of consent has been extended

  A set of fine-grained privacy preferences that define the actions that are permitted to be performed on a personal data item or a group of personal data items

- 3 use cases are considered
  - Employee data
  - Biobank
  - Assisted living

Context

Needs

– Increase of the proportion of elderly people

J-M Bockel, The situation of elderly persons in Europe, Council of Europe, 2007

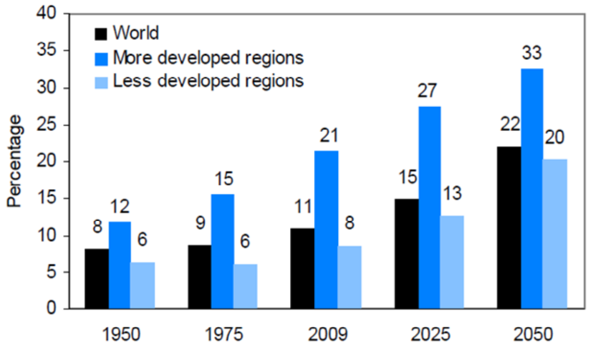
- 600 million people aged over 60 worldwide in 2007
- 1200 million in 2025
- 2 billion in 2050

– Increase in non-transmissible & age-related illnesses

- Senile dementia
- Parkinson's disease
- Locomotor disorders
- Alzheimer's disease
- Etc.

– Need for adapted care infrastructures

Figure 9. Proportion of population aged 60 or over: world and development regions, 1950-2050



http://www.un.org/esa/population/publications/WPA2009/WPA2009_WorkingPaper.pdf

Context

Needs

- Assisted living applications are expected to allow
  - The provision of care remotely
  - Elderly people to stay longer in their house
- Assisted living & the Internet of Things
  - Assisted living applications rely on sensors located on medical objects, e.g., thermometers
  - Medical sensing objects can communicate between themselves and with devices in other networks
  - In its action plan of 2009, “Internet of Things — An action plan for Europe”, the Commission Of The European Communities specified that IoT is expected to help meeting the challenges of an ageing society by allowing the deployment of health monitoring systems

Context

Personal Data Management and Security

- Provision of assisted living services requires processing personal data
  - Sensed by medical sensing objects (or sensing equipments)
  - Exchanged through the wireless link with service providers, between sensing equipments, etc.
- European regulation requires personal data to be processed with data subjects’ consent
  - E.g., EU Directive 95/46/EC
  - E.g., UK Data Protection Act
- Sensing equipments’ communications must be secured to avoid unauthorised entities to access data subjects’ personal data

Context

Personal Data Management and Security

Many of the previously proposed solutions do not provide

- Mechanisms to automate the enforcement and management of data subjects’ consent
- Access control management and the management of personal data through their entire lifecycle
- Dynamic provision of security services

Problem statement

How to

- Allow individuals to specify their consent for the use of each personal data item sensed by medical sensing equipments?
- Automate the enforcement of data subjects’ consent and the control of the access to data subjects’ personal data?
- Provide data subjects with an easy method to set up their consent and the security parameters allowing the secure exchange of their personal data?

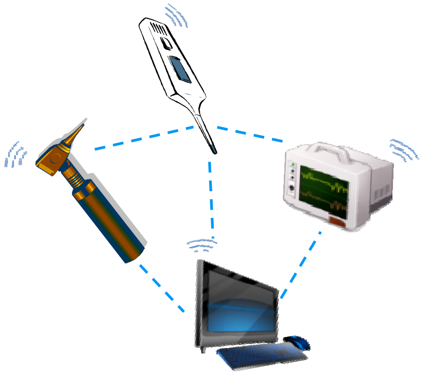
Scenario

Devices

Communication Box

- Stores the data sensed by the sensing equipments
- Manages the security of communications
- Controls the access to the sensed personal data

Sensing equipments



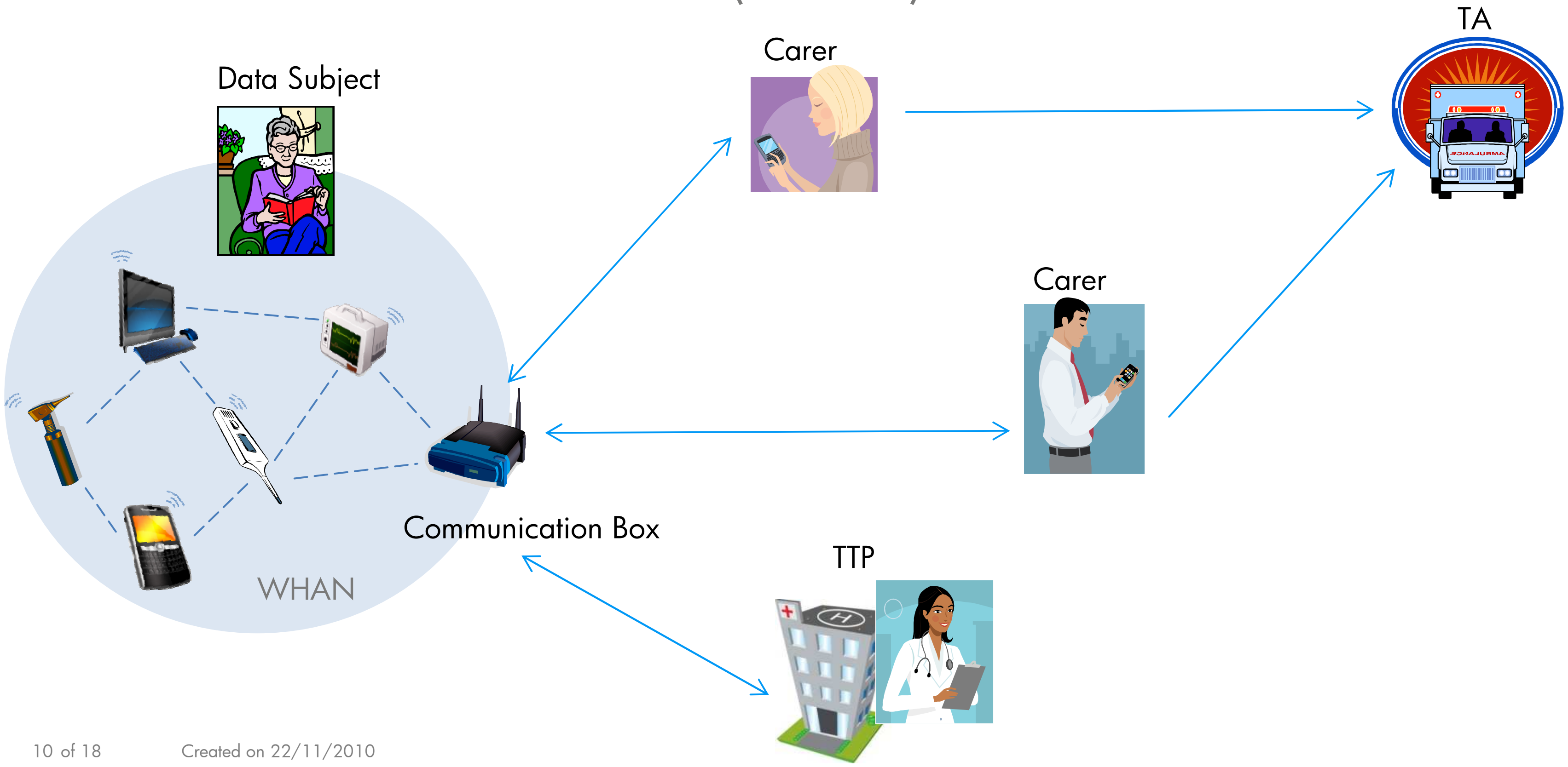
- Send measurements to the communication box
- May communicate between themselves

Administrator's device

- Has an application permitting to configure the communication box and distribute security parameters
- Has an application guaranteeing the privacy-aware management of personal data

Scenario

Wireless Home Access Network (WHAN)



Solution

Assumptions

– Sensing equipments’ capabilities

- Wireless interface, e.g. 802.11
- Near Field Communication (NFC) interface
- Equipped with a public key, e.g. Diffie-Hellman public key
- Generate and manage secret keys
- Store an identifier
- Receive and execute some commands, e.g. store session key, update session key, etc.

– Communication box’ capabilities

- Wireless interface, e.g. 802.11
- Manage cryptographic keys and personal data
- Establish secure communication channels
- Control access to resources

Solution

Assumptions

- Capabilities of the administrator’s mobile device
  - Wireless interfaces allowing the device holder to be constantly online
  - NFC interface
  - Application guaranteeing that personal data are only used as specified by the data subject
- TA’s capabilities
  - Equipped with devices running the application guaranteeing that personal data are only used as specified
  - Guarantees the proper management of personal data in emergency cases

Solution

Registration

At registration

– The data subject and his/her carer(s) specify who will administer the WHAN

After registration

– Each administrator is provided an administrator's device with smartcard containing

- The device's public/private key pair
- The communication box's public key
- The TTP's public key

– A communication box is provided which contains a smartcard with similar parameters

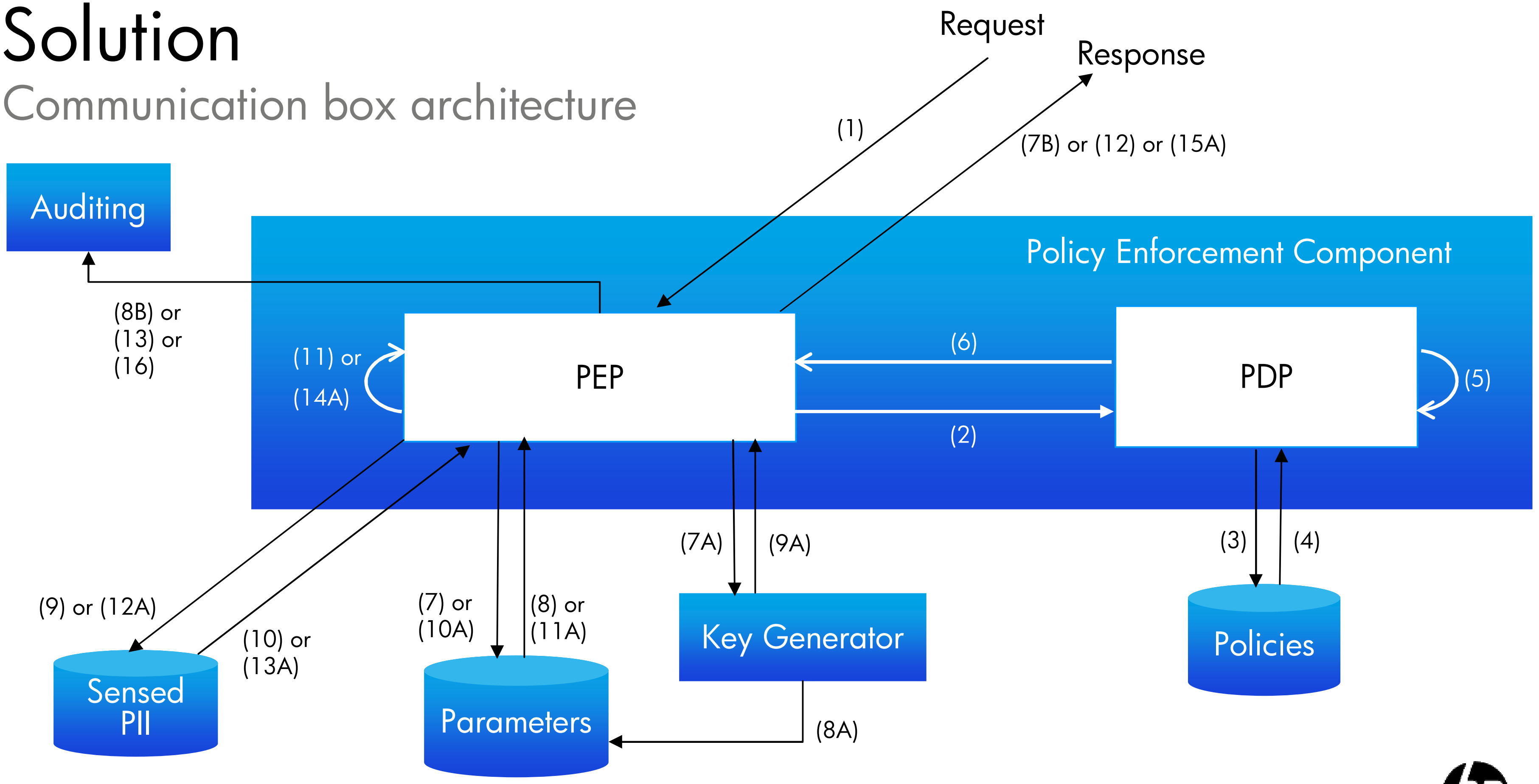
Solution

Initialisation of an equipment E with the configuration application on the administrator's device

- Identifier distribution and long term secret establishment
  - The configuration application generates an identifier ID_E and a Diffie-Hellman public key
  - A physical contact is established between the administrator's device and E
  - The contact allows to send ID_E to E and to establish a shared Diffe-Hellman secret key
- Specification of the policy and other parameters
  - Selection of the security policy which will secure E's communications
  - Specification the data subjects' privacy preferences = Consent for the use of the data sensed by E
- Transmission of the parameters to the communication box
  - The specified parameters are sent to the box through a secure communication channel
  - Transport Layer Security (TLS) can be used to establish a secure channel

Solution

Communication box architecture



Solution

Maintenance

- The TTP regularly verifies the state of the communication box to guarantee that it operates properly
- The communication box parameters are regularly securely backed up at the TTP to allow their access if the communication box is out of service
- In case of technical problem requiring the communication box to be collected by the TTP's technical team
  - An administrator's device temporarily acts as communication box
  - The administrator' s device is securely transmitted the backed up parameters
  - After the communication box has been repaired, the administrator's device removes the parameters and stop acting as a communication box

Conclusion

- The proposed approach shows how IoT can allow meeting the challenges introduced by the ageing society
- The proposed approach automates the protection of individuals’ privacy, based on their consent
- It allows individuals to easily set up and manage their WHAN
- It makes maintenance transparent to individuals
- Future work
  - Implementation
  - Evaluation
  - Extension of the solution to cover, amongst other, compliance with the data protection laws

Privacy-Preserving Management of Personal Data For Assisted-Living Applications

Gina Kounga, Marco Casassa Mont, Pete Bramhall
Researcher

29 November 2010