Passive Sensor Nodes
Are they meaningful without protection?

IFIP WG 11.2 : Seminar 2010

Manfred Aigner
IAIK, TU Graz

Available Documents

BRIDGE project: Sensor-enabled RFID tag handbook

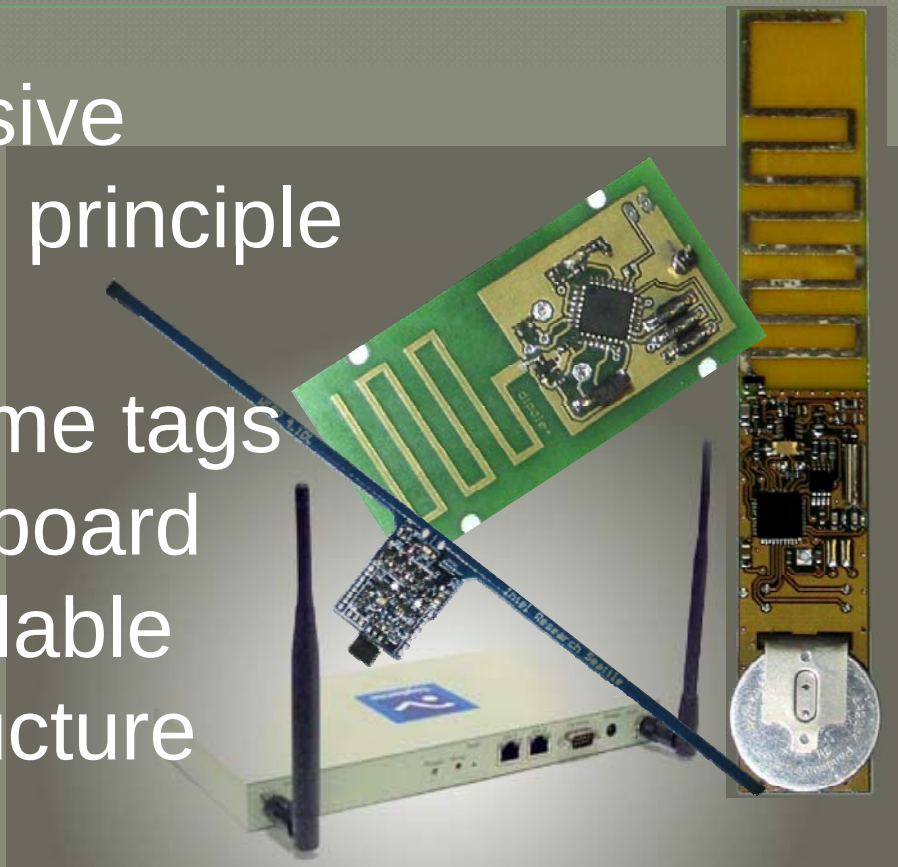
ToC:

- Introduction
- State of the art
- Wireless sensor data communication
- Features and Requirements of sensor enabled RFID tags
- Ambient intelligence with sensor-enabled RFID tags
- Real life pilot project with sensor enabled tags

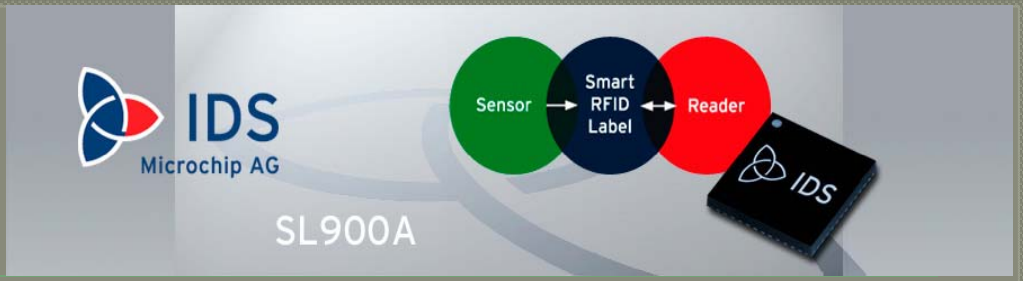
…no security mentioned…

Passive sensor nodes?

- Passive or semi-passive
- RFID communication principle (reader triggered)
- Low cost – high volume tags
- Simple controller on board
- Compatible with available RFID reader infrastructure also NFC
- UHF and HF



Products



SL900A Datasheet

EPC Class 3 Chip with Sensor … is an EPC Class 3 tag chip …track, monitor, time-stamp and record information about any goods in any supply chain or cold chain transport. …healthcare and environmental supervision…

Description:

.. in semi-passive mode … as well as in fully passive mode.

Key Features:

Frequency: 860 to 960 MHz (UHF)

Data logging from:

- On-chip temperature sensor
- External sensors

On-chip 9k-bit EEPROM

Anti-collision capability

Security features mentioned:
Chapter 6.10 Data Protection (of SL900A)

Additional to the Gen2 lock protection, [..] offers read/write protection using 3 password sets for 3 memory areas. Each 32-bit password is divided into 2 16-bit passwords, where the lower 16 bits are reserved for the Write protection and the higher 16 bits are reserved for the Read/Write protection.

Pictures & data taken from product‘s webpage

Products: GENTAG

- DatasheetA - Datasheet B
- GT-301: **Overview**
  - Available either as passive or battery-assisted logging sensors
  - Wireless temperature sensing combined with unique ID
  - Standard industrial sensing range from –20 ºC up to +60 ºC ±0.5 ºC
  - Custom 0.1 ºC technology available (diagnostics)
  - HF 13.56 MHz ISO 15693 compatible
- No security features described

Pictures & data taken from product‘s webpage

Products: Melexis

- Datasheet:
  - Versatile A/D interface for resistive sensors
  - ISO-15693 13.56MHz transponder
  - Slave / Master SPI interface
  - 4 k-bit EEPROM with access protection
  - Standalone data-logging mode
  - Ultra low power
  - Battery or battery-less applications
- Security mentioned:

The user data are separated in 8 pages, whose access levels (L0 to L3) are defined thanks to 2 bits, stored inthe '*Security Map Register' of the EEPROM. A security procedure based on a password is required to* execute the unlocking. The password is stored in EEPROM #06 (16 bits ~ page 24).

Pictures & data taken from product's webpage

CAEN

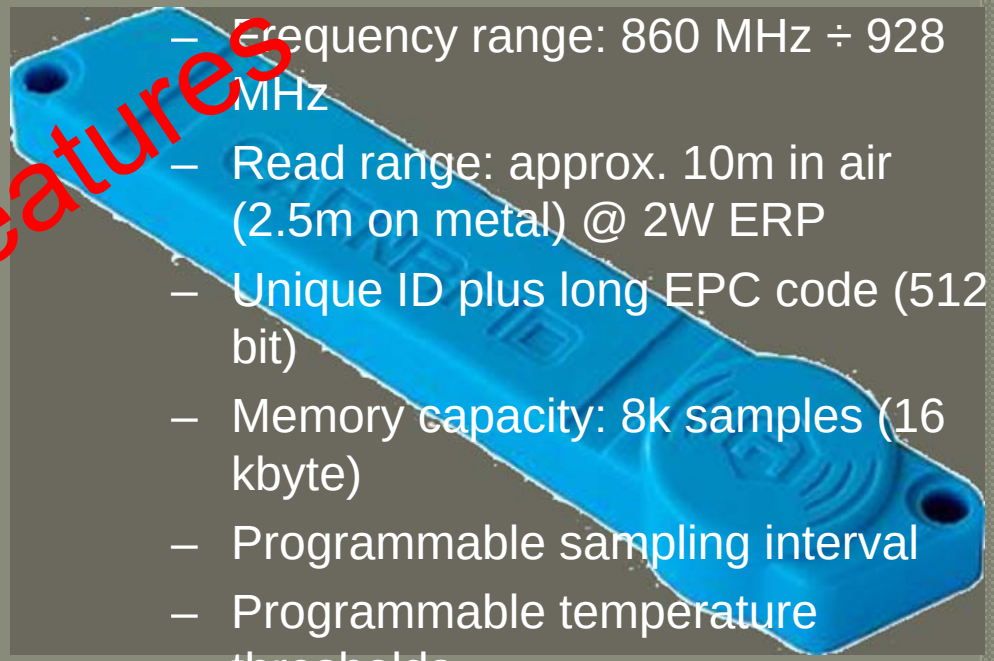
Temperature Logger: RT0005

- Highlights EPC C1G2 (ISO18000-6C) Compatible
- Frequency range: 860 MHz ÷ 928 MHz
- Read range: approx. 10m in air (2.5m on metal) @ 2W ERP
- Unique TID plus long EPC code (512 bit)
- Memory capacity: 4k samples (8 kByte)
- Multiple programmable sampling interval
- Multiple programmable temperature thresholds

no security features described

Semi passive Logger A927Z:

- EPC C1G2 (ISO18000-6C) Compatible
- Frequency range: 860 MHz ÷ 928 MHz
- Read range: approx. 10m in air (2.5m on metal) @ 2W ERP
- Unique ID plus long EPC code (512 bit)
- Memory capacity: 8k samples (16 kbyte)
- Programmable sampling interval
- Programmable temperature thresholds
- Battery life: 3 or 5 years
- Battery charge measurement through RF



Pictures & data taken from product‘s webpage

Use case – Cold Chain Surveillance

- Central server with application (e.g. cold chain surveillance)
- Fact: Tag travels in unprotected/non-trusted zone
- A.) Tag enters trusted zone to be read out
- B.) Tag sends its data via a trusted reader through internet to server
- C.) Tag sends its data via non trusted reader to server
- D.) Tag never leaves trusted zone (useless for many applications)

Cold Chain Surveillance: Who do we trust?

- The shipping warehouse?
- The delivery service?
- The receiving warehouse?

It depends who checks the sensor‘s data!

Cold Chain Surveillance: Who is able to attack an RFID tag

- E.g. a sleazy trucker wants to hide his failure before delivering the goods …

Possible attacks

- Guess password (16 bit passwords!!)
- Spoof password when tag operates with reader
- Read data out
- Modify data after reading
- Modify data when stored on the sensor
- DPA (still an overkill)
- Fault attacks (what for?)

Mentioned application areas (Product datasheets)

- Healthcare (Fever measurement, Temperature monitoring of medical products)
- Cold chain monitoring and tracking
- Asset management and monitoring (security and integrity), Pharmaceutical logistics
- Building automation
- Industrial, medical and residential control and monitoring
- Dynamic Shelf Life applications

Things to do …

- Raise awareness of protection in sensor community
- Analyze possible use cases
- Develop and suggest protection concepts that fit to applications, assuming that tags travel in non trusted areas

Activities @ IAIK

- WISP – Wireless Sensor Platform from Intel labs

…Paticipate at "WISP Challenge"!!!.. @ google (WISP INTEL)

Ongoing activities

- ISO/IEC/IEEE WD 21451.7
  Information technology — Smart Transducer Interface for Sensors and Actuators — Transducers to Radio Frequency Identification (RFID) Systems Communication Protocols and Transducer Electronic Data Sheet Formats

… suggests AES for authentication and encryption of sensor data.