RAIN RFID V2+Crypto
Conformance and Performance Testing

Josef Preishuber-Pflügl
CTO, BU Manager RFID+RFComm
j.preishuber-pfluegl@cisc.at

October 2015
CISC Semiconductor

Independent - CISC was founded in 1999 and is a 100% private owned company

Experienced - CISC is managed by an international team of highest skilled experts & working with RFID for more than 18 years

Global - we serve the whole industry worldwide
About CISC RF

- Team of **RFID professionals** with long-term, international reputation
- **Performance improver** of RFID products and systems through our solutions
- **Measurement tool provider** for RFID and NFC conformance, performance and interoperability tests
- **Standardization leader** in RFID
CISC Role in RFID Standardization (Excerpt)

- Convener ISO/IEC SC31 WG4/S6 RFID Performance and Conformance test methods
  - ISO/IEC 18046 RFID performance
  - ISO/IEC 18047 RFID conformance
- Co-chair GS1 EPCglobal TLRPP Tag Label Reader and Printer Performance
  - Static performance test
- Co-chair GS1 EPCglobal UHF AI Group
  - EPCglobal UHF Gen2V2 air interface
  - EPCglobal UHF Gen2V2 conformance tests
- Project editor ISO/IEC 18000-63 Type C
- Project editor ISO/IEC 29167-1 Crypto
IOT – Internet of Things
RFID and NFC providing the

- Last mile / kilometer
- Last yard / meter
- First meter
UHF RFID

RAIN RFID

GS1 EPCglobal Gen2

ISO IEC 18000-63
UHF RFID Air interface standards

- EPC Gen 2 = ISO/IEC 18000-63 Type C
- EPC Gen 2V2 = ISO/IEC 18000-63REV1
- Crypto extensions = ISO/IEC 29167
- Brazil derivatives
  - SINIAV G0
  - ARTESP PA
  - Brasil-ID P63

Published 20 Oct 2015
What’s NEW - EPC Gen2V2?

- Crypto solution for even more applications (e.g. road tolling)
- European privacy concerns addressed (Untraceability command)
- File management available for more data with different owners (Different ownership)
NEW, but not Gen2V2 specific

- Mature products in high volume
- Better tag sensitivity
  - Read range continuously increased (> 20 m)
  - Area surveillance (> 1000 m$^2$)
  - Movement direction detection

- …
Difference Gen2 V1.2.0 – V2

Mandatory
Gen2 V2
ISO/IEC 18000-63REV1

Gen 2 V1.2.0
ISO/IEC 18000-63:2013
ISO/IEC 29167 Crypto Suites

- ISO/IEC 29167-10 AES128 ✓
- ISO/IEC 29167-11 PRESENT80 ✓
- ISO/IEC 29167-12 ECC-DH ✓
- ISO/IEC 29167-13 GRAIN128 ✓
- ISO/IEC 29167-14 AES128-OFB like ✓
- ISO/IEC 29167-15 XOR
- ISO/IEC 29167-16 ECDSA-ECDH ✓
- ISO/IEC 29167-17 Crypto GPS ✓
- ISO/IEC 29167-19 RAMON ✓
- ISO/IEC 29167-20 Algebraic Eraser
- NP 29167-21 Simon
- NP 29167-22 Speck
Test standards

- ISO/IEC 18046-1 System performance
- ISO/IEC 18046-2 Interrogator performance
- ISO/IEC 18046-3 Tag performance
- ISO/IEC 18047-6 Tag and interrogator conformance
- GS1 EPCglobal Tag Performance Parameters and Test Methods v 1.1.2
- GS1 EPCglobal US TIPP
Testing

- Tag
  - Conformance
  - Performance

- Reader
  - Conformance
  - Performance

- System
  - Efficiency
  - Interoperability
UHF RFID Tag Test Procedure

- Reader independent test
  - Use tag identification & read commands
  - Use reference reader
    (close to ideal = no tag response missed)
  - Write commands
- Attach tag to a product or reference material
- Test tag performance over the whole range of UHF frequencies allocated for RFID
- Test tag performance over the whole range of power levels
- Performance of tags attached to various spots of the products
Frequency Dependent Sensitivity

- Tag turn on power over the frequency band
  - Frequency-dependency of the tag design
  - Impact of the tagged object on the tag performance
Orientation degradation of tag sensitivity

How can you read the tag from the various sides?
Fully automated conformance test

Does the tag meet the standard requirements?
Conformance Test Results

- New Crypto commands of ISO/IEC 29167
- New EPC Gen2V2 and ISO/IEC 18000-63REV1
Reader testing (Tag Emulation)
Reader signals

Check the waveforms:
Well filtered, smooth, no spikes, ...
Communication details
Understand and analyze the command stream

* Command: [Select] - Start timestamp (us): 284008012 - Stop timestamp (us): 284009599
  Target: Inventoried (S0)  Action: Matching: assert SL or inventoried -> A;
  Non-Matching: deassert SL or inventoried -> B  MemBank: EPC  Pointer: 32  Length: 0
  Mask: - Truncate: Disable truncation  CRC-16: OK
* Response: none -------------------

* Command: [Query] - Start timestamp (us): 284010226 - Stop timestamp (us): 284011272
  DR: DR=64/3  M: M=2  TRext: Use pilot tone  Sel: All  Session: S0  Target: A  Q: 2
  CRC-5: OK
* Response: none -------------------

* Command: [QueryRep] - Start timestamp (us): 284011689 - Stop timestamp (us): 284011902
  Session: S0
* Response: none -------------------

* Command: [QueryRep] - Start timestamp (us): 284012916 - Stop timestamp (us): 284013130
  Session: S0
* Response: none -------------------

* Command: [QueryRep] - Start timestamp (us): 284016565 - Stop timestamp (us): 284018179
  RN: BD9D  CRC-16: OK
* Response: RN = 51CB  CRC-16 = B759  CRC OK -------------------

© CISC Semiconductor GmbH | www.cisc.at
System Test
Understand the environment

Quick check:
Is there any other (disturbing) application around?
Query with high Q

Quick check:
Is the reader working efficient – Lots of empty slots?
Get EPC with FM0

FM0 backscatter
⇒ Only 2.5 ms for one EPC/UII
Get EPC with M=4

Miller M= 4 backscatter

⇒ Increased to 5 ms for one EPC/UII
Xplorer—The versatile RFID test equipment

Performance tests

Conformance tests

Reader tests

In-lay testing

Tag Emulation
IoT’s **FIRST** meter as key success factor

Finding the lost bits in seconds instead of days

Know **how** to place, track and manage your **tags and readers**

Pass all tests for full certification

Save time and money for the user
Visit us at www.CISC.at