RAIN Radio Protocol

December 2015

RAIN RFID

Background

RAIN reader–tag communications use the UHF Gen2 radio protocol. The MIT Auto-ID Center pioneered the early work on the UHF Gen2 protocol in 2002, transitioning the effort to EPCglobal, a subsidiary of GS1, in 2004. EPCglobal ratified V1.0.9 of the Gen2 protocol in Dec. 2004, followed by V1.1.0 in Dec. 2005 to fix errata. In May 2008, EPCglobal ratified V1.2.0, a backward-compatible update to V1.1.0 with new optional features and commands for item tagging. Gen2 V1.2.0 is known colloquially as V1.

In Sep. 2007 Walmart, Best Buy, Tesco, Metro, C&A, Target and others formed a JRG (joint requirements group) within EPCglobal to investigate using Gen2 for electronic article surveillance (EAS). This JRG produced an EAS requirements document in Aug. 2008, at which time the retailers created another JRG to develop requirements for consumer privacy, brand protection, and securely altering a tag's memory contents in the field (collectively Tag Alteration or TA). This TA JRG ratified its requirements in Nov. 2009. In Aug. 2010, the EPCglobal Consumer Electronics Industry Action Group published its Item-level Tagging (ILT) Requirements which included a need for large user memory that could be partitioned into logical regions (i.e. files). EPCglobal then undertook to add the EAS, TA, and ILT capabilities to the Gen2 protocol, ratifying the revised protocol, Gen2 V2.0.0, in Oct. 2013 and V2.0.1 (to fix errata) in Apr. 2015. Gen2 V2.0.1, known colloquially as V2, is a backward-compatible* enhancement to V1 that supports loss prevention (EAS), brand protection, security, files, and consumer privacy.

ISO standardized Gen2 V1.1.0, V1.2.0, and V2.0.1 as ISO/IEC 18000-63, with each new version superseding the prior one. ISO published V2.0.1 as ISO/IEC 18000-63:2015 in Oct. 2015.

The changes between V1 and V2 are solely logical, meaning they affect reader commands, tag replies, data structures and memory usage but do not alter the waveforms a reader or a tag send over the air.

Gen2 V1

V1 specifies the core requirements for the radio and logic layers of RAIN communications.

Radio layer

V1 specifies a passive-backscatter, reader-talks-first RFID radio operating in the 860–960 MHz frequency range.

A reader transmits information to a tag by sending a modulated radio signal. A tag receives energy and information from this radio signal. Although V1 only defined requirements for passive tags (i.e. those that receive their energy solely from the radio signal), it did not preclude battery-assisted passive-backscatter tags that receive some or all of their energy from a battery, nor did it preclude sensor-enabled tags. ISO/IEC 18000-63 extended V1 to cover battery-assisted passive-backscatter and sensor tags.

A reader receives information from a tag by sending a continuous-wave radio signal; the tag modulates its antenna reflectivity to backscatter an information signal to the reader. Sending data by modulating an antenna's reflectivity is called *passive backscatter*. A tag backscatters data only after being instructed to do so by a reader.

*There are a few incompatibilities between V2 and V1, noted below. Considering the minor nature of these incompatibilities, the GS1 Gen2 working group determined it had met its mandate of delivering a V2 protocol that was backward compatible with V1.

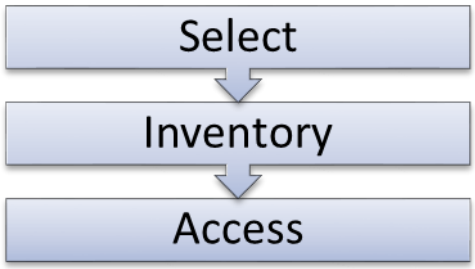
Logic layer

V1 specifies that readers manage tag populations using three sequential operations

a) **Select.** Choosing a tag population. A reader may select one or more tags based on a value or values in tag memory. A reader may subsequently inventory and access the chosen tag(s).

b) **Inventory.** Identifying individual tags. A reader initiates an inventory round. One or more tags may reply. The reader detects a single tag reply and requests the tag's EPC.

c)



Access. Communicating with an inventoried tag. The reader may perform a core operation such as reading, writing, locking, or killing the tag. A reader may only access an inventoried tag.

Gen2 V2

V2 enhances V1 Select and Access, preserving the sequential nature of the operations.

Radio layer

The V2 radio is unchanged from V1.

Logic layer

The V2 logic layer enhances the V1 logic layer with the additions shown in italics.

a) **Select.** Choosing a tag population. A reader may select one or more tags based on a value or values in tag memory*, and may challenge one or more tags based on tag support of a cryptographic suite and authentication type*. A reader may subsequently inventory and access the chosen tag(s).

b) **Inventory.** Identifying individual tags. A reader initiates an inventory round. One or more tags may reply. The reader detects a single tag reply and requests the tag's EPC.

c) **Access.** Communicating with an inventoried tag. The reader may perform a core operation such as reading, writing, locking, or killing the tag*; a security-related operation such as authenticating the tag; or a file-related operation such as opening a particular file in the tag's user memory.* A reader may only access an inventoried tag.

These changes to Select and Access enable the following new V2 functionalities:

- **Loss prevention:** V2 enables tag-based EAS, in which codes stored in tag memory indicate whether the item to which the tag is attached is (1) store-owned or foreign and (2) sold or unsold.
- **Brand protection:** V2 enables cryptographic tag authentication.
- **Security:** V2 enables secure tag access and secure communications between reader and tag.

- **Files:** V2 enhances user memory with support for memory files and file privileges.
- **Consumer privacy:** V2 allows hiding portions of tag memory, reducing tag read range, or both.

All of these new functionalities are optional, meaning that a supplier may implement one or more of the features depending on the needs of the applications.

As is proper for a radio protocol, V2 does not specify how a tag or a reader implement loss prevention, brand protection, security, file management, or consumer privacy. Instead, it provides reader commands, tag replies, data structures and memory which suppliers can optionally use to implement these functionalities.

Several of the new V2 features may employ cryptographic algorithms, for example for brand protection, security, or consumer privacy. V2 does not specify which cryptographic algorithm a tag uses; instead, V2 supports a range of algorithms, leaving the choice to the supplier. ISO/IEC 29167 has ratified or is in the process of ratifying more than ten cryptographic algorithms to date. V2 anticipates a tag will support only one algorithm (although it allows a tag to support more than one) but readers will support many. V2 also allows readers not to support any algorithms and instead funnel all cryptographic communications from a tag to a network or cloud host, and vice versa.

Backward compatibility

V2 is considered backward compatible with V1. However, to enable V2 functionalities and address unresolved V1 issues, V2 introduced the following incompatibilities.

1. **Replace recommissioning:** To enhance consumer privacy V1.2.0 added features to V1.1.0 allowing an end user to alter a tag's memory (i.e. recommission a tag) at point-of-sale. V2 replaced tag recommissioning with more-capable tag untraceability and tag security. The Gen2 working group verified that recommissioning was not field-deployed in any RAIN tags before replacing it.
2. **Modify protocol-control (PC) bits:** When a tag backscatters its EPC it also backscatters PC bits that tell a reader useful information like the EPC length, whether the tag is attached to a hazardous item, and whether the tag has user memory. In V1.1.0, many PC bits were "reserved for future use" (RFU). With each successive protocol version the working group used more PC bits, optionally extended the PC length when needed. For example, in V2.0.0 the working group added a bit that tells a reader if the tag is killable. The working group also refined how a tag implements a few of these bits. For example, to improve tag usability V1.2.0 added a feature whereby a tag, when sending its EPC, also asserted a user-memory indicator (UMI) bit if user memory existed and contained data. To satisfy the GS1 IP policy, in V2 the UMI bit solely indicates whether user memory exists.
3. **Enhance memory locking:** To improve tag usability Gen2 V1.2.0 added the ability to permanently lock blocks of user memory against subsequent overwriting. V2 enables TA EAS by allowing a successive memory locking operation that was previously disallowed.

Since V2 ratification, a few fielded systems have reported an issue from incompatibility #2. To date, there has only been a single issue, but more incompatibilities could arise when tags implement optional PC bits that were RFU and set to zero in prior versions of the protocol.

The single identified issue involves the UMI bit. Although V2 highlighted the issue, its root cause is a backward incompatibility between V1.2.0 and V1.1.0. Specifically, V1.1.0 readers, when encoding tag EPCs, do not expect an asserted UMI bit, and may fail if the UMI bit is asserted. V1.2.0 tags assert their UMI bit if user memory exists *and* contains data; fortuitously, pre-encoded tags rarely had data in user memory so the UMI bit was deasserted, meeting the expectations of V1.1.0 readers (note that the issue would have undoubtedly surfaced at some point). V2 tags assert their UMI bit if user memory exists, so V1.1.0 readers saw an asserted UMI bit and some failed the encoding. To date, this issue has been resolved with reader firmware updates.

Conclusion

The Gen2 radio layer is unchanged across V2.0.1, V1.2.0, and V1.1.0. The V2.0.1 logic layer enhanced the V1.2.0 logic layer by adding support for loss prevention, brand protection, security, file management, and consumer privacy. The V1.2.0 logic layer, in turn, enhanced the V1.1.0 logic layer by adding support for item tagging. These logic-layer enhancements are all backward compatible (with the minor deviations noted above), are all optional, and all extend the type and range or applications that Gen2 can support. Consequently, the RAIN Alliance will use either (i) Gen2, (ii) ISO/IEC 18000-63, or preferably (iii) the RAIN radio protocol when referring to all versions of UHF Gen2.

ABOUT RAIN RFID ALLIANCE

The RAIN RFID Alliance is an organization founded in April 2014 to promote awareness, increase education and support the universal adoption of UHF RFID technology. RAIN members are manufacturers, distributors, resellers and researchers working with the EPC Gen2 UHF RFID specification, incorporated into the ISO/IEC 18000-63 standard.

RAIN RFID is a wireless technology that connects billions of everyday items to the Internet, enabling businesses and consumers to **identify**, **locate**, **authenticate** and **engage** each item. For more information, visit www.RAINRFID.org.

The RAIN RFID Alliance is part of AIM Global, the worldwide authority on automatic identification, data collection and networking in a mobile environment. AIM is dedicated to accelerating the growth and use of Automatic Identification and Mobility technologies and services around the world. For more information, visit www.aimglobal.org.

RAIN® RFID

Association for Automatic Identification and Mobility

RAIN RFID

One Landmark North
20399 Rte 19
Cranberry Twp., PA 16066

If you're interested in having your company become a member of RAIN or have any questions about the RAIN alliance, please send RAIN an e-mail: info@rainrfid.org