Published June 1, 2003. Distribution restricted to Sponsors until September 1, 2003.

TECHNICAL REPORT

Compliance and Certification: Ensuring RFID Interoperability

Tom A. Scharfeld

AUTO-ID CENTER MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 400 TECHNOLOGY SQ, BUILDING NE46, 6TH FLOOR, CAMBRIDGE, MA 02139-4307, USA

ABSTRACT

In order for RFID to successfully penetrate into large open systems, RFID interoperability is a necessity. Not only must tags from any vendor be able to communicate with readers from any vendor, but a given tagged object must be able to be identified by readers of any user in a wide variety of application conditions. As a key first step the Center has developed protocol standards. Protocol standards, however, are not enough – information about product capabilities, expected levels of performance, and assurance that products, if applied correctly, will be interoperable, are also necessary. A properly designed compliance and certification program can address these issues and lay the groundwork for ensuring RFID interoperability. This paper describes the relevant elements of an RFID system implementation and presents options and recommendations for a compliance and certification program for the Center.

Published June 1, 2003. Distribution restricted to Sponsors until September 1, 2003.

TECHNICAL REPORT

Compliance and Certification: Ensuring RFID Interoperability

Biography

Tom A. Scharfeld
Program Manager

At the Center, Tom Scharfeld is researching RFID technology, applications, and their standardization. His current work involves developing methods for evaluation of readers, tags, and their performance in system implementations. He rejoins the Center after having spent a year at NTT's Wireless Systems Innovation Laboratory in Japan developing an active-tag based object locating system. His previous work at the Center was focused on low-cost passive RFID. He has previously worked at Northwestern University's Laboratory for Intelligent Mechanical Systems on minimalist robots capable of complex object manipulation, and Panasonic Factory Automation on high- speed chip placement machines. Tom has a Master's from MIT and a Bachelors' from Northwestern University, both in Mechanical Engineering.

Published June 1, 2003. Distribution restricted to Sponsors until September 1, 2003.

TECHNICAL REPORT

Compliance and Certification: Ensuring RFID Interoperability

Contents

1. INTRODUCTION

RFID has traditionally been implemented in closed systems by a single integrator for a single user or a tightly controlled community of users. The Center is driving away from this towards enabling the implementation of RFID in large open systems. This can only be realized if tags from any vendor are able to communicate with readers from any vendor, and a given tagged object can be identified by readers of any user in any of the wide variety of possible application conditions it may encounter. In short, not only must tags and readers be interoperable, but more specifically, tagged objects and their aggregations must be interoperable with readers and their unique installations. This defines RFID interoperability. RFID interoperability is a key goal for the Center and its community.

Towards achieving RFID interoperability, the Center has developed open standard protocols with base functionality at three standard frequencies. These standard protocols should encourage multiple vendors to produce interoperable devices leading to increased competition among vendors and more and better options for users.

However, three main problems emerge:

1. the user will need some assurance that products truly conform to the specifications.
2. the standard has options – end users will need to know which options a product supports.
3. protocol standards on their own are not enough – in order to realistically set expectations and make important system design decisions, information regarding performance and/or minimum performance standards will also be necessary.

A properly designed compliance and certification program could address all of these problems.

After briefly reviewing the important elements of an RFID system implementation, this paper presents options and recommendations for a compliance and certification program for the Center.

2. ELEMENTS OF AN RFID SYSTEM IMPLEMENTATION

Regardless of whether we are a vendor developing technologies, a user trying to satisfy the needs of their application, or a standards developer trying to control the vendors and users, we are all focused on one thing: the RFID system implementation. This section will briefly review the components of an implementation, the frequencies, protocols, functionality, and performance that they control, the participants that create and use the components, and the overall process.

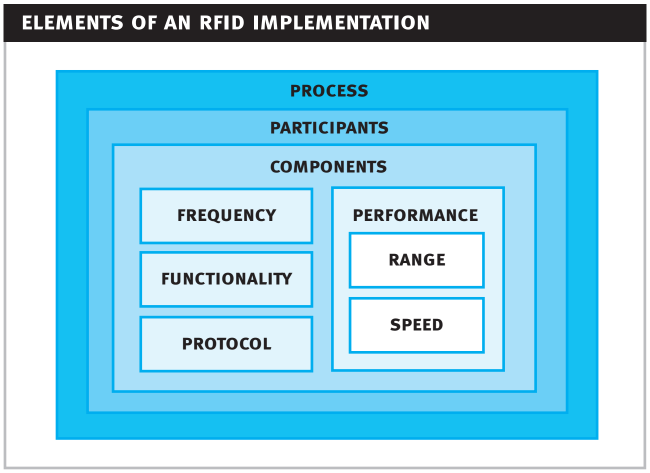


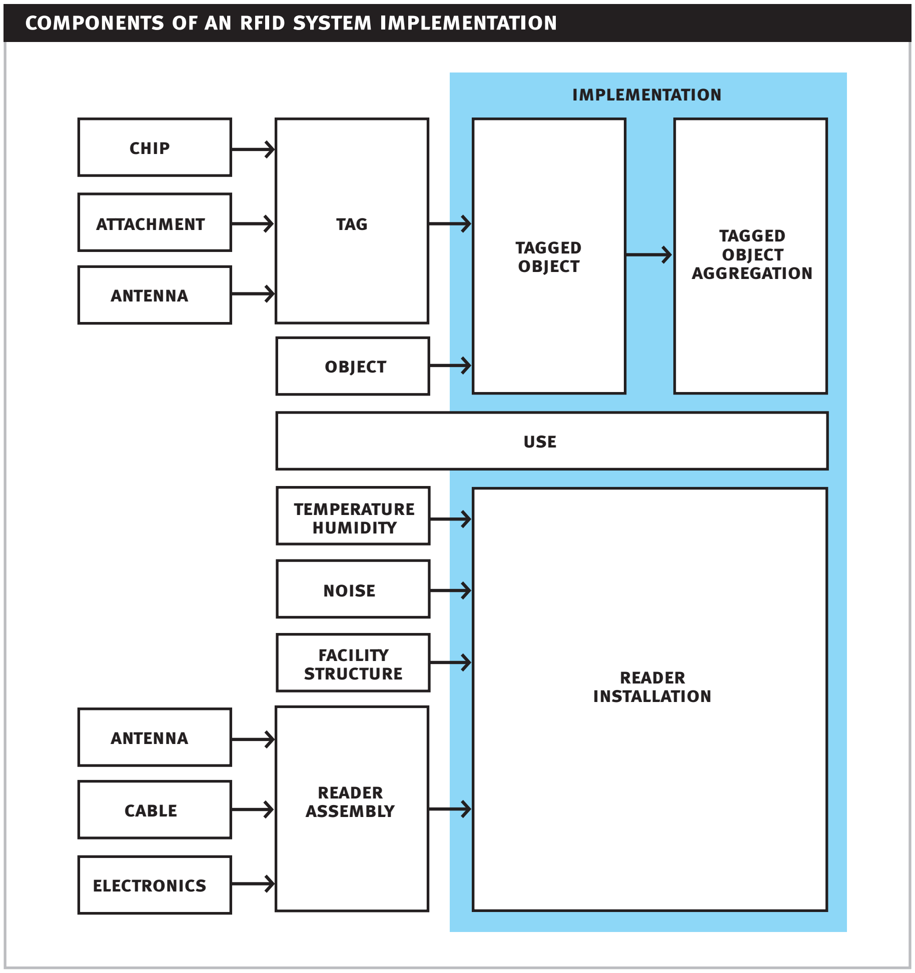
Figure 1: The process describes the way the Participants interact. The Participants create and use the Components. The Components control Frequency, Functionality, Protocol, and Performance.

2.1. Components

Very generally, an RFID system implementation is a merging of RFID technology with the intended application. The technology consists of tags and readers. The application consists of the objects to be identified, the environment, both physical and electromagnetic, and finally the use dynamics. The components of an RFID system implementation are shown in Figure 2.

Figure 2

COMPONENTS OF AN RFID SYSTEM IMPLEMENTATION



Tags are composed of chips attached to an antenna on some substrate. Tags are applied to objects to create tagged objects. In this process, the object itself comes part of the antenna. Tagged objects can also be combined in groups to create tagged object aggregations. Tagged items, cases, and pallets are all examples of tagged objects. The items within cases, and the cases on pallets are examples of tagged object aggregations.

Readers are composed of electronics and antennas. In many cases antennas are separated from readers and modular. This is often the case for fixed readers. In other cases, antennas are integrated directly within the reader. This is typically the case with mobile readers. Reader installations are created when reader systems are confined to facilities and their environments. The environment consists of physical aspects such as structures, machines, and people as well as temperature, humidity and pressure. It also consists of electromagnetic noise.

Tagged objects and tagged object aggregations traverse facilities and their reader installations. The participants controlling these various components are discussed in section 2.2. The process by which they are created and used is discussed in section 2.3.

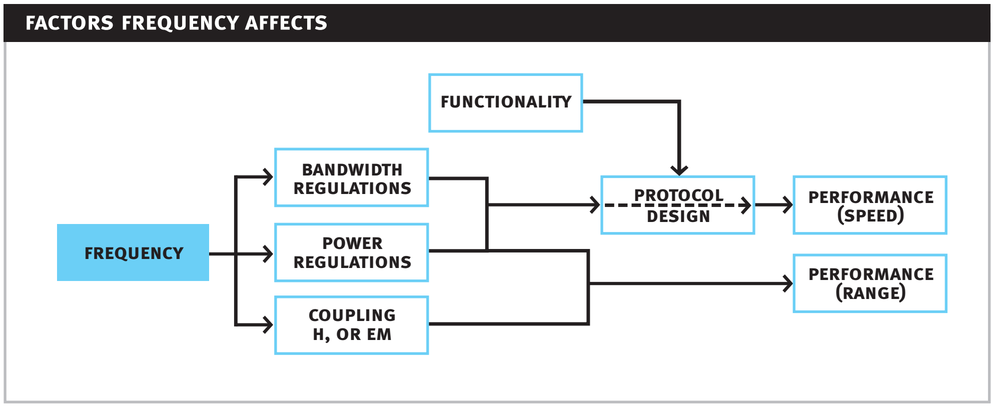
Though neatly decoupled in the diagram, in actuality, every component is strongly coupled. Predictability of performance from system components has not been demonstrated. However, just as different participants control different system components, different components control different system capabilities and behaviors. These consist of frequency, functionality, protocol, and performance elements such as range and speed. We will briefly review how each component contributes to and controls these attributes.

2.1.1. Frequency

Frequencies are especially important to RFID systems as they determine power and bandwidth regulations, and the method of coupling between reader and tag. Power regulations are a lead contributor to range. Bandwidth regulations are a lead contributor to speed. Together they influence the design of the protocol. Passive RFID systems operating in HF frequencies typically rely on coupling via magnetic-field, whereas those operating at UHF frequencies rely on coupling via radiated electromagnetic waves. Coupling method is a lead contributor to performance – in particular, range.

Figure 3

FACTORS FREQUENCY AFFECTS



Frequency is controlled by the tag chip and antenna, and the reader electronics.

2.1.2. Functionality and Protocol

Functionality refers to the capabilities of the tag. For the most minimal tags, this consists of memory and anti-collsion capability. Some tags are read-only and others are read-write. Other functionality includes more memory, sensors inputs and actuator output. Functionality is wholly controlled by the tag chip and reader electronics.

Protocols are the languages by which tags and readers are able to communicate. They consist of multiple layers: an RF layer, and a command layer. The RF layer converts baseband digital signals to and from RF signals capable of transmission through the wireless channel. Readers, as the master devices, have an anti-collision algorithm for distinguishing multiple tags within a reader’s field. Readers direct the communications; tags respond (ideally) consistently to commands.

The protocol is also largely controlled by the tag chip and reader electronics. Attachment, cabling, antennas, and propagation can influence timing parameters.

The Auto-ID Center's tag class structure, classifies tags on the basis of protocol and functionality for three standard frequencies [1][2][3][30]. These are summarized in table 1.

Table 1: NOTE: Darkly shaded boxes indicate that the protocol has not yet been formally defined.

AUTO-ID CENTER TAG CLASS STRUCTURE

	HF	UHF		
			MW	
	13.56 MHz	868/915 MHz	2.45 GHZ	
Class 5	▨	▨	▨	Active, TBD
Class 4	▨	▨	▨	Active, TBD
Class 3	▨	▨	▨	Semi-Passive, TBD
Class 2	▨	▨	▨	Passive, TBD
Class 1				Passive, read-write, EPC™ -only
Class 0	▨			Passive, read-only, EPC™ -only
Coupling	**H-field**	**EM**	**EM**	

2.1.3. Performance

Key performance variables are range and speed. This section gives a briefly overview of the factors contributing to and affecting range and speed. A more through explanation can be found in [4]. Some factors contributed by readers can be found in [5]. A review of some antenna types can be found in [6].

2.1.3.1. RANGE

Range is determined largely by power. Power is transmitted and received by electronics, through attachment and cabling, distributed through space via antennas, and attenuated and shielded through the wireless channel. Range is affected by every component of the RFID system implementation and consequently highly unpredictable. Some of these factors are summarized in table 2:

Table 2

SOME CONTRIBUTIONS OF RFID SYSTEM IMPLEMENTATION COMPONENTS TO RANGE	
Chip	power rectification, consumption, modulation
Attachment	loss
Tag Antenna	UHF: gain, pattern (beamwidth), polarization HF: number of loops, area, materials, etc.
Object	detuning, shielding, no reception (via orientation and location)
Reader Electonics	power transmission (via regulations and frequency)
Cabling	reflection and loss
Reader Antenna	UHF: gain, pattern (beamwidth), polarization HF: number of loops, area, materials, etc.
Structures	fading (large-scale and small-scale)
Noise	noise power relative to signal power
Temperature/Humidity	propagation loss
Dynamics	change in orientation, location

2.1.3.2. SPEED

Assuming the tag is within range of the reader, speed (identification rate), is largely determined by frequency bandwidth, protocol, the reader's anti-collision algorithm, number of tags within the field, and noise. Signal timing is also an important component. An additional factor which can slow identification rate is unexpected response of readers and tags to momentary power loss to the tag.

Given its dependency on protocols and algorithms, speed is largely determined by the reader electronics and the tag chip. Environmental noise and number of tags within the field are the other key components. Cabling, attachment, antennas, and environmental variables can affect timing parameters resulting in poor signal quality and erroneous transmission, slowing speed.

2.2. Participants

There are a number of participants involved in the creation and use of an RFID system implementation.

In the tag manufacturing and application chain, these include:

- chip companies focused primarily on manufacturing chips,
- tag companies responsible for designing chips and antennas,
- assemblers and converters who manufacture antennas and create tags,
- packaging companies, or other applicators who apply tags to objects

In the reader manufacturing chain, entities include:

- reader design and manufacturing companies
- antenna design and manufacturing companies
- integrators who install reader systems for users

Users include:

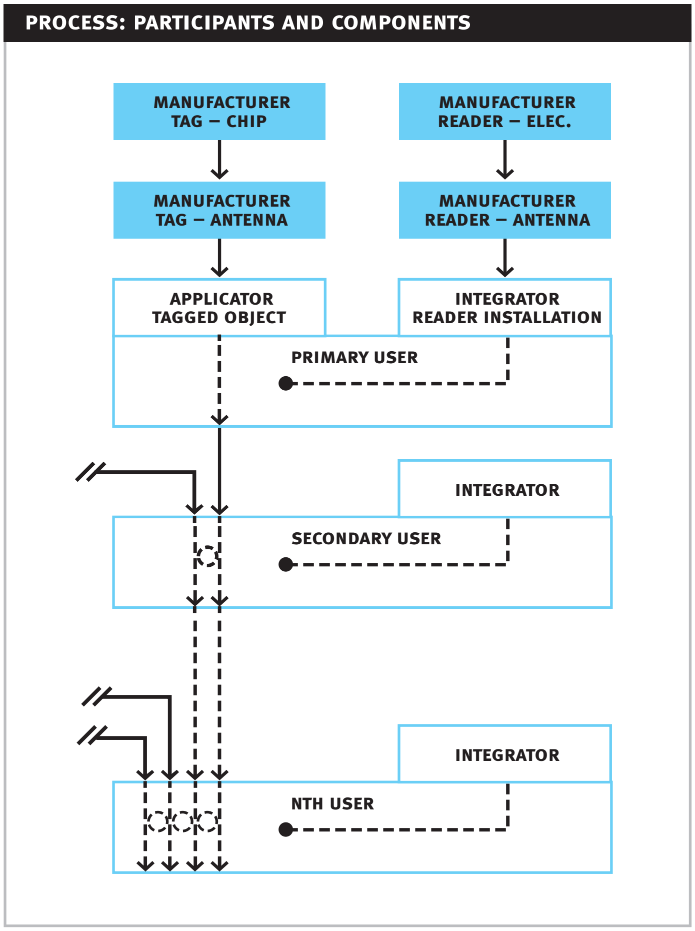
- manufacturers
- distributors
- retailers, and eventually
- offices, homes, and recycling centers

Each participant has responsibility for the products that they design and manufacture. Users, as well, have responsibility for the tagged objects, and tagged object aggregations that they create and distribute. In one sense they are supplying a technology to users downstream. Accountability of the individual entities is especially important when considering compliance and certification.

2.3. Process

The participant involved in the creation and use of an RFID system implementation and all of its components are shown in the simplified model of Figure 4. Tagged objects are the base units that travel through the facilities of all users downstream. Aggregation of tagged objects may remain unchanged or may be de-aggregated and aggregated into different groups by individual users. Reader installations remain fixed to facilities. It should be expected that users downstream in the chain will see consolidation of a variety of different objects with a variety of different tag types.

Figure 4


PROCESS: PARTICIPANTS AND COMPONENTS
MANUFACTURER TAG – CHIP
MANUFACTURER READER – ELEC.
MANUFACTURER TAG – ANTENNA
MANUFACTURER READER – ANTENNA
APPLICATOR TAGGED OBJECT
INTEGRATOR READER INSTALLATION
PRIMARY USER
INTEGRATOR
SECONDARY USER
INTEGRATOR
NTH USER

The model shown in Figure 4 represents a radical departure from the way RFID systems are installed and used today. Today it is common for integrators to install an entire system consisting of tags and readers for a single user. Often the tags will remain within the four-walls of a particular facility, or travel within a tightly controlled supply-chain. Migrations from the current process to that shown in Figure 4 will require a higher degree of modularity between tags and readers. The compliance and certification program must address this.

2.4. Summary

A summary of the components of an RFID system implementation, who creates them, uses them, and what attributes they affect, can be found in Appendix A. In summary, there are a number of points we must keep in mind when creating a compliance and certification program.

Regarding the individual components of an RFID system implementation,

- There are options within the Auto-ID Center's standards in frequency, protocol and functionality.
- Frequency, functionality and protocol implementation are largely controlled by the tag chip and reader electronics.
- Range is determined by every component of the RFID implementation, in particular the tag, object, reader, antennas, and attached structure.
- Speed is largely determined by the anti-collision algorithm for the particular protocol, the population of tags within the field, and noise.

In regards to the participants and process:

- A large number of participants compose the RFID system manufacture and use chain. Each is responsible for the component they design and manufacture.
- Tagged objects are the base units that travel throughout the supply chain.
- Consolidation of tag types occurs downstream – users must know what to expect.
- Migration toward use of RFID in large open systems will require a higher degree of modularity between readers and tags.

Given these key points, in order to best facilitate RFID interoperability and rapid adoption of RFID in large open systems,

- For evaluation purposes, components should be isolated from other components wherever possible.
  - This allows for accountability of the various participants for their respective components.
  - It also allows for the isolation of the components and their contributions to frequency, functionality, protocol and performance. This won't result in proving interoperability at any one stage, but chances may be improved at each stage.
- Isolation is important, but true interoperability can only be tested in an actual implementation.
- Given the options in frequency, functionality, and protocol, information must be made available to users so they know what to expect and how best to design their system.
- Standards and information are useful, guidlines on such topics as how to install readers, and how to stack pallets, may also be necessary. This, however, is beyond the scope of this paper.

3. OPTIONS FOR COMPLIANCE AND CERTIFICATION

Now that we have reviewed the elements of an RFID implementation and how they pose problems to RFID interoperability, the chief goal of the compliance and certification program, we will evaluate the Center's options. We will begin with an introduction to compliance and certification and then examine its role at the Center. We will recommend a process, discuss test types, environments, and equipment, and finally present options for evaluating compliance of the various system components.

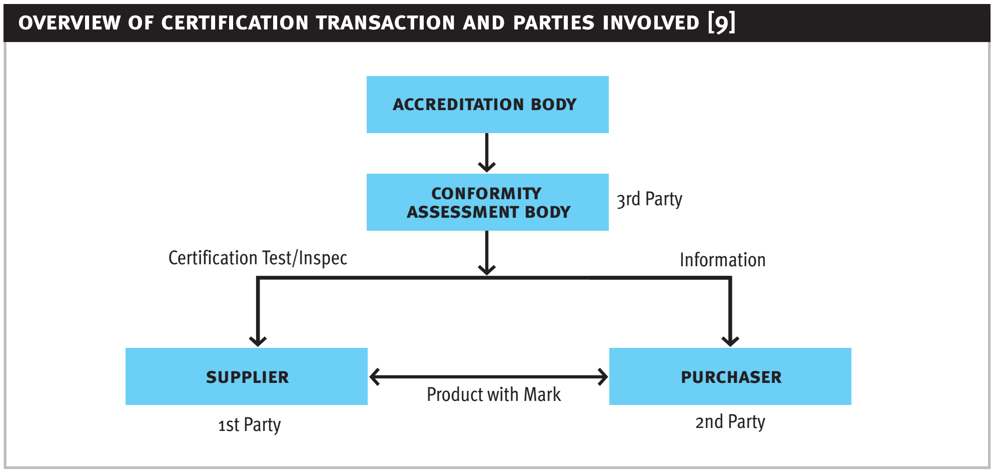
3.1. Introduction to Certification

Certification is formally defined as a "procedure by which a third party gives written assurance that a product, process, or service conforms to specified requirements [7]". This written assurance could come in the form of a certification mark or labeling applied to a product, or to its documentation, and/or listing in a publicly accessible registry. As defined by ISO, it falls into a class of "conformity assessment," which includes not only product certification, but also general testing and inspection, verification, accreditation, and other related activities [8]. Figure 5 illustrates the role of conformity assessment among the three parties of a transaction.

Conformity assessment is defined as "any activity concerned with determining directly or indirectly that relevant requirements are fulfilled [7]".

Figure 5

OVERVIEW OF CERTIFICATION TRANSACTION AND PARTIES INVOLVED [9]



In general, three parties take part in conformity assessment activities and may perform the conformity assessment themselves. The first party is the supplier or vendor of a product or service. Conformity assessment by the supplier is often referred to as self-declaration of conformance (SDoC). The second party, is the purchaser or user of a product or service. They often perform their own evaluations if no other formal procedures exist. Finally, there is the 3rd party which is an organization independent of both the supplier and end user. 3rd party conformity assessment activities can be regulatory or voluntary. Regulatory assessment is typically performed for proving adherence to safety code.

In certification, the brand and associated trademarks are of extreme importance. Not only can they provide the basis for legal enforcement of requirements and sanctions against participants, but they embody attributes and features of the product and program. It is the brand and mark which the purchasing party sees and requests.

3.2. Compliance and Certification at the Center

In order to assure the purchaser of a product, whether it be a packaging company purchasing a tag, or a user downstream accepting an aggregation of objects, that it will function, the Center should establish a certification program. Given the number of participants affected by a single tag on a particular object and its application by a single participants at a single point in time, process and procedures must be in place to provide assurance to all users that tagged objects can be identified. Users must know what types of tags to expect and their level of performance. This will provide the basis for guidance on how to install their reader systems, and whether or not they should make use of auxiliary systems (physical or virtual) to improve system reliability.

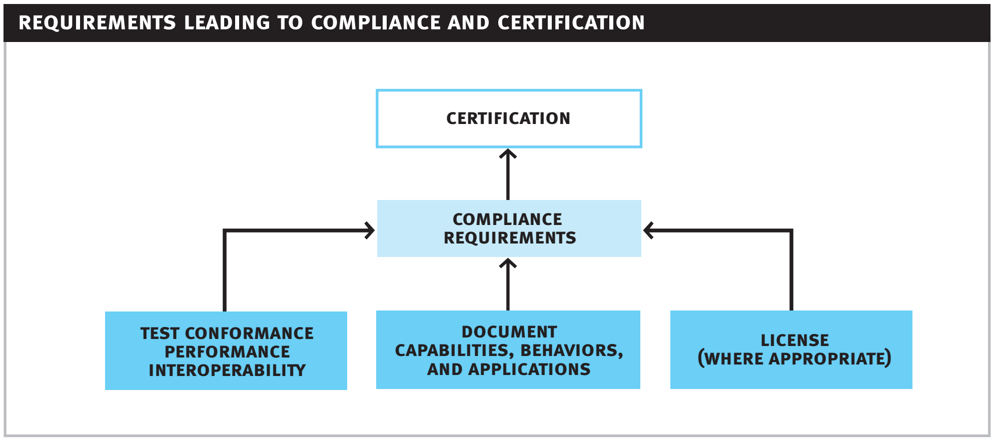
Table 3: Compliance goals for participants of RFID production and use chain

1ST PARTY		2ND PARTY		GOAL
Chip Co.	prove compliance to	Tag Co.	that	Chip conforms to specs
Tag Co.	prove compliance to	Applicator	that	Tag is appropriate for object
Applicator	prove compliance to	Users	that	Tagged object is readable everywhere
Users	prove compliance to	Users	that	Tagged object and aggregations are readable
Reader Co.	prove compliance to	Integrator	that	Reader electronics conform and antenna ok
Integrator	prove compliance to	User	that	Installation will read all tags

In order to qualify for certification, a product must be deemed compliant. We will use the term "compliance" to indicate that key requirements, such as testing, documentation, labeling, and potentially, legal requirements have been met. Figure 6 shows the proposed overall requirements leading to compliance and certification.

Figure 6

REQUIREMENTS LEADING TO COMPLIANCE AND CERTIFICATION

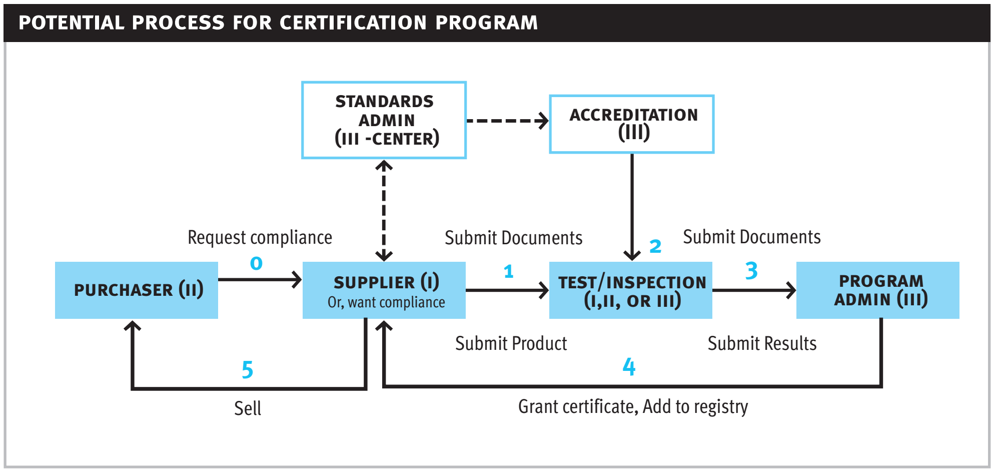

CERTIFICATION
COMPLIANCE REQUIREMENTS
TEST CONFORMANCE PERFORMANCE INTEROPERABILITY
DOCUMENT CAPABILITIES, BEHAVIORS, AND APPLICATIONS
LICENSE (WHERE APPROPRIATE)

3.2.1. Certification Process

Given the complexity of the RFID system and nature of the supply chain, single entities play both 1st and 2nd party roles. Users may not only purchase and apply tags, but they also distribute them on objects to users downstream. However, we can expect that certification will follow a similar process regardless of the component one is supplying or using. A potential process is diagrammed in Figure 7.

Figure 7

POTENTIAL PROCESS FOR CERTIFICATION PROGRAM



The general process begins by the purchaser either requesting that the supplier sell compliant products, or the supplier itself desiring compliance for marketing purposes (step 0 in Figure 7). The process ends by the supplier selling the product to the purchaser (step 5 in Figure 7). The recommended certification process itself consists of the following four steps:

1. The supplier should submit documents detailing the capabilities, behaviors and intended applications of the product. Depending on the product, capabilities could include such parameters as frequency, functionality, and protocol. This should be done for all products ranging from chips and electronics through tagged object aggregations and reader installations. Documentation is briefly discussed in section 3.2.2.

2. The appropriate test should be performed – conformance, performance, or interoperability – in the appropriate conditions, with the appropriate equipment. The test could be performed by the supplier, the vendor, the Center, or another 3rd party. Test types, environments, equipment, and performers are discussed in section 3.2.3.

3. The test results along with the original supplier's documentation should be submitted to a program administrator – most likely the Center, or possibly another 3rd party.

4. Finally, if the results and documentation are sufficient, a certificate could be granted, allowing the official right to claim Auto-ID or EPC-compliance. The product along with relevant information from the documentation could be registered in the certified products registry.

NOTE: Quality inspections may follow a slightly different process.

3.2.2. Documentation

Given the options available in the standard, and the variables constituting performances, documentation plays an important role. It is particularly useful at three main stages:

1. testing – supported options, capabilities, and intended applications should be noted in order to facilitate efficient testing

2. selection – given the options in the standard, the various grades of performance, and the complexity of large open systems, information on supported options, capabilities, intended applications and grades of performance should be made available to users

3. standards setting – useful and appropriate standards can only be set based on valid information about technologies, applications, their implementations.

Forms of documentation include implementation conformance statements (ICS), and/or intended application statements (IAS) to be submitted at the time of testing or inspection, and finally results from the tests themselves. Appropriate parameters from all forms of documentation may be included in an online registry of certified products, systems, and personnel (for example, integrators). This could be publicly accessible or limited to key users. Some information could be kept confidential and limited to the standards administrator.

Submittal of implementation conformance statements (ICS) is standard practice for conformance testing, particularly for testing communications systems [10]. Online registries are also widely used.

3.2.3. Testing

In general, testing should isolate the parameters intended to be measured. Tests should be repeatable, reliable, and reproducible so that multiple facilities in a number of geographic locations may perform tests. Further, we must keep in mind the general tradeoff between coverage and cost. The more exhaustive the test, the likelier it is to have a higher cost [10].

Before describing procedures and tests for individual components in more detail, it will be useful to consider the various options for testing, including test types, test environments, and test instrumentation and equipment. Though independent of the above, we will also briefly discuss options for test performers.

3.2.3.1. TEST TYPES

As previously described, there are three broad categories of tests we should consider:

- Conformance tests
- Performance tests, and
- Interoperability Tests

Conformance tests should be designed to test individual parameters and actual operations against the specifications. Testing both individual parameters and actual operations will depend on the circumstances, but generally the more redundancy in the test, the better that a device may conform, leading to improved interoperability. For example, test of reader electronics may check modulation timing parameters specifically, in addition to running an entire transaction between reader and automated test instrumentation or tools. Generally, results would be pass or fail.

Performance Tests could include testing of individual parameters, such as tag sensitivities, and tagged object radiation pattern and polarization. They should also include testing performance of various operations; for example, the reader's tag identification rate under various populations of tags, with differing levels of noise, and other simulated conditions. Though currently no formal performance standards exist, this is under review. Regardless, the tests should be performed and results should be submitted for listing in the registry. Where necessary, certain parameters may be kept confidential.

Interoperability tests are those where actual systems are tested against other actual systems. Tagged objects and aggregations of tagged objects could be tested in actual reader installations, or in reader installations as close to actual conditions as possible. Tests would normally be pass/fail, but with proper instrumentation could also reveal specific performance parameters for diagnostic purposes.

Conformance, performance, and interoperability tests are commonly performed for certification of many communications systems. For example, cellular phones [22][28] and Bluetooth-supported devices [17] undergo conformance tests that evaluate conformance to elements of the supported protocol. WiFi, Bluetooth, and GSM phones undergo interoperability tests that evaluate devices in conditions more closely resembling the actual application – whether it be actual operation of full devices in lab conditions as in the case of WiFi [21], actual operation of protocol profile software in the case of Bluetooth [16], or actual operation of handsets in the vicinity of a sample of actual base stations as in the case of GSM [26].

Though these tests are commonly performed, in all cases, the actual scope, purpose, and definitions of the tests vary; Bluetooth conformance and interoperability tests are very different from GSM conformance and interoperability tests. This should be expected given that the technology, applications and their maturity are all very different. Our definitions are appropriate to the current and desired state of RFID.

3.2.3.2. TEST ENVIRONMENTS

Test environments may take one of three main forms:

- Standard Laboratory Conditions
- Application Reference Conditions
- Application Field Conditions

Their suitability for a particular test will depend on the purpose of the test.

Standard laboratory conditions are well-calibrated and well-known conditions. They may include anechoic chambers, open air test sites. GTEMs, shielded enclosures, or direct wired connections. For UHF antenna measurements, the anechoic chamber is the preferred environment. For testing of chips and electronics, direct wired connections are the preferred environment.

Application Reference Conditions could be those where common applications are simulated. For example, they may simulate portals, conveyors, forklifts, pigeon holes, etc. These conditions have not yet been specified. Further, because they are not repeatable, reliable, reproducible, and representative of actual field conditions, the other test environments should be considered first.

Application Field Conditions are actual use conditions. Though not repeatable, reliable, and reproducible, they are most indicative of what a particular tagged object, or aggregation of tagged objects may encounter. Such conditions may be useful for interoperability tests. A broad cross section of appropriate conditions could be selected for testing of particular tagged objects and aggregations. Selections could be made based on “intended application” information recorded in the product registry for reader installations and tagged objects.

Ultimately the chosen test environment must reflect the purpose of the test and the component being tested. Most conformance and many performance tests occur in well-calibrated laboratory conditions. Such is the case with CTIA’s cellular phone protocol testing program [27], Bluetooth [17], and WiFi [21]. In the case of the Global Certification Forum for interoperability certification of GSM, the actual field environment is used [26].

3.2.3.3. TEST EQUIPMENT

Test equipment may also take one of three main forms. It may include:

– Standard test equipment
– Validated test tools
– Actual devices

Standard test equipment includes all standard, well-calibrated test equipment and instrumentation. This includes instrumentation such as oscilloscopes, spectrum analyzers, network analyzers, and signal generators. It also includes, calibrated antennas, cabling, RF components, and positioners. Use of this equipment will result in the most repeatable and reliable results, and will be widely reproducible. Also, output parameters are in well-known and widely used engineering parameters, useful for input into existing models.

Validated test tools are tools and test devices that may repeat ably and reliably perform the expected functions. These could be considered reference devices. Reference readers and tags could be constructed. They could allow for a higher degree of control, capture of certain data parameters, and well-calibrated measurements. The downside is that such devices will need a calibration and validation procedure of their own. However, given the efficiency they should bring to conformance and performance testing – increasing coverage, while decreasing time and cost – they should be well worth the investment.

Actual devices may also be used as test reference devices. This would be most appropriate for actual interoperability tests. However, if testing a reader’s identification rate for very large populations of tags, it may be feasible to build large assemblies of pre-validated tag IC chips.

For testing of other technologies, existing standard test instrumentation is most widely used. Yet in many technologies, particularly communications devices, special testing instruments and systems are created. For testing of wireless protocols, such as GSM, CDMA, Bluetooth, and 802.11b a number of special test instruments are available. Typically these become available after the market has achieved sufficient maturity, or promises maturity within a certain timeframe. In the case of Bluetooth, test instruments are available for testing both software and RF hardware [13]. Some are provided for design, development and production testing, whereas other systems are used for certification. For certification of Bluetooth software, validated profile testers are used. For certification of Bluetooth RF hardware, a system consisting of a validated Bluetooth tester in addition to other standard test equipment is used [15].

In addition to test instrumentation, other test tools can be useful. In the case of RFID, dummy objects or actual objects may be required to evaluate tagged object performance. The CTIA, in their cellular phone handset certification program requires testing of the handset against a dummy head filled with a fluid of known dielectric [28].

3.2.3.4. TEST PERFORMERS

In addition to determining test requirements and methods, test performers and program/documentation administrators must also be identified.

There are four general options for test performers:
- Create own 3rd party lab.
- Accredit 1st party
- Accredit other 3rd party labs
- Contract process to a single 3rd party lab to manage

Creation of its own lab would allow the Center the greatest degree of control, yet would require the most resources. Further, accessibility by global customers could prove to be difficult.

At the other extreme, the Center could chose to accredit the vendor themselves to do the test. This approach may be most efficient, yet would provide the minimal level of assurance to the user. Further, suppliers would need to be individually inspected and accredited, adding additional complexity to the problem.

Another option is accreditation of other 3rd party labs. Though still requiring an accreditation process, and sacrificing the efficiency of a 1st party test, a high degree of assurance would be provided to the user. Further, expertise and global access of existing 3rd party labs could be leveraged.

The final option is to contract the testing and certification program to a single independent 3rd party. Benefits may vary with the particular lab. In exchange for an exclusive contract, cost to the Center could be minimal. Global locations may also be available.

All approaches are in practice. The WiFi Alliance has contracted its process to a single global certification lab for management of both the testing and its overall process [21]. The Bluetooth Special Interest Group has establishg a test facility qualification program for accreditation of either 1st parties or independent 3rd party labs [13]. The CTIA also qualifies independent 3rd party labs [27]. Cable Labs has chosen to create their own lab for certification of cable modems.

3.1.4. Options for Component Testing and Compliance

Now that we have described the overall certification process, the various test types, test conditions, and equipment, we will consider options for testing and documentation of the various RFID implementation components in more detail.

Conformance and Performance tests in well-calibrated conditions with well-calibrated instruments are suggested where possible and where useful. Interoperability tests of the actual system – including tagged objects and tagged object aggregations with reader installations – are suggested to verify interoperability. Testing options for chips, tags, tagged objects, tagged object aggregations, readers, antennas, cables and reader installations are discussed. A summary of these options is included in Appendix B.

3.2.4.1. CHIPS

Evaluation and certification of the chip should be an option as the chip essentially controls the protocol implementation as well as certain key performance variables. It would provide assurance to all tag designers, converters, and assemblers that the chip will function. Finally, it could serve to speed the evaluation process for tags, tagged objects, and finally aggregations of tagged objects.

Chips should be submitted with a statement declaring supported frequencies, functionality, and protocols.

The chip could be tested in one of two ways:

1. through a 50 ohm matching circuit with coax connection; or,
2. through attachment to a pre-determined and validated reference antenna design.

The first option could likely be carried out in typical ambient conditions. The device under test would be attached directly through coaxial cable (with appropriate RF components) to the test system. The second option could require an anechoic chamber, open field, shielded box, or other environments depending on frequency and desired test parameters and output. It is expected that the first option would be the more repeatable and reliable of the two.

Equipment used for testing could include:

1. standard test equipment (signal generator, spectrum analyzer w/IF out to digitizer, etc.) with GPIB interfaces and computer control.
2. validated test reader.

Since the chip contains the data, controls the functionality and protocol and contributes to operability at particular frequencies, conformance to the protocol specifications should be tested. All RF parameters such as frequency, timing and power should be tested. In addition, response to all commands and preferably sequences of commands should be tested.

Performance parameters should also be tested. These parameters could include sensitivities for basic identify, read, and write operations, as well as the level of modulation back to the reader. Resistance to noise might also be tested in this configuration, either through addition of a signal generator transmitting pre-defined noise patterns, or additional readers. Also, the chips ability to maintain power in the event of a momentary loss of power should be checked.

Finally, results should be well-documented. If the device passes the appropriate tests, it should be listed in the registry. Supported frequencies, protocols, and functionality should be listed. Key performance variables may also be listed.

3.2.4.2. TAGS AND TAGGED OBJECTS

The main purpose of the tag test (assuming the chip has already been certified) is to check its antenna performance on the intended object. Testing of tags on objects is a crucial step towards providing assurance not only to a single user, but every user downstream of them, that the object can work within their system.

In applying tags, we may have to satisfy the following situations:

– antenna designed specific to objects
– antenna designed for classes of objects (based on materials, or applications)
– antenna designed for generic application

Given the variation in performance based on the object to be tagged, the variety of possible tag application scenarios, and the importance of achieving good performance.

The tag should be submitted with a statement, outlining,

1. capabilities of the chip (its frequency, protocol, and functionality, and certification record, if available),
2. expectation of performance
3. intended application conditions (types of objects, placement on the objects, and the conditions under which it will be used).

If the tag is designed for a specific object, the entire object should be tested (packaging, as well as materials). If it is designed for a broad class of objects (based on materials and applications), representative objects should be included for the test. If it is designed for generic applications, the tag should be tested with a set of dummy objects having different conductivities (metal box, box with liquids of different dielectrics, and paper, for example).

The test environment will preferably be an anechoic chamber, or open field. Test equipment should include turntable and positioners to automate collection of pattern, orientation and polarization data. Appropriate reference antennas and probes will be necessary. Horn and log periodic antennas may be suitable for UHF measurements, whereas loop antennas or magnetic field probes may be suitable for HF measurements.

As in the case of the chip test, test instruments could include:

1. standard test instruments, such as signal generators, spectrum analyzers, network analyzers etc., with GPIB interface, signal correlation, and computer control
2. pre-validated test reader, or
3. a combination of the two

If the tag being tested contains a pre-certified chip, the data, functionality, and protocol may not need to be as thoroughly tested. The real focus of the tag/tagged object conformance and performance test is evaluation of the patterns and orientation sensitivities for the different operations of the tag: raw identification, read, and write. Requirements have not yet been set for these parameters, yet their knowledge may benefit standards administrators in standards setting efforts as well as potential users in system design efforts.

Finally, the results should be documented and made available in the product registry. Links to the pre-certified chip should be included, and frequencies, protocols, and functionality should be listed. Intended objects and applications should also be listed.

3.2.4.3. Tagged Object Aggregations

Wherever possible, tagged object aggregations should undergo the same test as tagged objects. In certain situations where pallets are mixed, an option may be interoperability testing of random samples of mixed pallets. Or, a system may be installed which notifies the receiving user of the percentage of cases that they can expect to read. This can be accomplished by providing the receiving user data gathered by the sending user for the particular mixed pallet. Such an option would give the receiving user an indication as to the degree to which they must rely on data aggregation and containment.

3.2.4.4. Readers

The purpose for certifying readers is to assure integrators that the readers they purchase,

1. have certain frequencies, functionality, protocols, and
2. perform well enough for the application.

Certification of readers allows the reader designers and manufacturers to be held accountable for the readers they produce. It allows the user to hold the integrator accountable for the system they install.

NOTE: The host/network interface must be addressed separately.

Readers should be submitted with a statement listing:

1. Frequencies, functionality, and protocols
2. Intended regions of operation
3. Intended and certified antenna parameters (and sample)
4. Performance expectations

Evaluation of the reader should consist of:

- conformance testing against the appropriate specifications,
- performance testing of individual RF, command, and algorithm layers, and
- performance testing of the ability to read various populations of tags,
  - the rate at which they're read, and how it is affected by
    - presence of noise from other readers,
    - simulated multi-path,
    - loss in power of tags, and
    - temperature variations.

Readers can typically be isolated from the antennas as they have standard 50 ohm outputs. In the case of handheld readers, antennas could be bypassed. Not only does this allow isolation from antennas, but it also allows isolation from environmental variables. Rather than attaching an antenna, the more repeatable, reliable, and reproducible approach is to create a test apparatus through coaxial connections to the test equipment.

Test equipment could consist of standard test instruments such as a spectrum analyzer with IF output to a digitizer for test of signal timing, and signal generators for simulating tag responses and noise. The instruments could be automated through GPIB interface and controlled by computer. Another option is to use validated test tags. These would be well-calibrated self-contained tags. They could be connected via coax cable. RF components and noise sources could be used to create large populations of tags with simulated path loss and noise. Noise could be generated via a signal generator or a dummy reader.

Given the complexity of readers, there are a large number of variables to test, ranging from individual parameters of individual subsystems (such as Rx and Tx), to full operation of the entire system. The following options exist:

1. Conformance and Performance via individual parameters

- Isolate RF section receive and transmit –
  - Tx – transmit standard bit patterns and check output with a spectrum analyzer w/IF output to digitizer
    1. Check frequency characteristics
    2. Check power output
    3. Check conformance of modulation timing parameters
  - Rx – check sensitivity of receiver with signal generator input (and additional un-wanted noise sources including other readers, or standard pattern)
- Commands – check existence and output of individual commands, output could be baseband, or RF output

2. Conformance and Performance via operability test with simulated reader from test equipment, or test tag assembly

- Check operability of single tag
- Check read rate with
  - Varying tag populations
  - Simulated noise
  - Simulated propagation loss and multi-path
  - Simulated loss of power to tag

The best combination of options will depend on cost of the test instrumentation and tools, cost of the test itself versus the level of coverage desired.

Finally, readers demonstrating conformance and a sufficient level of performance (when that is determined) should be listed in the registry. Listing should include all capabilities and important performance characteristics.

3.2.4.5. ANTENNAS AND CABLING

Antennas and cabling are key components of the system. In many cases their characteristics are already measured and documented. In certain cases, there may be no need for additional testing. Standard measures for antennas include, pattern, polarization, gain, and antenna factor. Standard measures for cabling includes loss per unit distance and voltage standing wave ratio (VSWR) of connectors.

In cases where custom antennas and assemblies are designed for a particular reader, the entire assembly should be tested, and parameters such as gain, pattern, and polarization should be measured, documented, and listed along with the reader. This may be necessary for handhelds and other mobile readers.

3.2.4.6. READER INSTALLATIONS

In installing a reader system, there are a variety of options. These include,

- Types of readers – frequencies, functionality, protocols (not to mention networking capability)
- Types of antennas – number and arrangement

In order to make the proper selection, a number of factors must be taken into account:

- Types of tags expected (their frequencies, functionality, protocols, and performance)
- Arrangements of tagged objects
- Environmental components (structures, noise, temperature/humidity, dynamics)

Given the complexity, one option may be to certify or accredit the integrator themselves. In performing the installation, the integrator may need to test the tagged object registry for expected tagged object characteristics, or perform their own interoperability tests with expected tagged objects and aggregations.

The integrator themselves should be able to submit the appropriate documentation to the program administrator for listing of the installation in the registry. Documentation could include application conditions and system capabilities.

3.2.4.7. INTEROPERABILITY TESTING: TAGGED OBJECTS, AGGREGATIONS, AND READER INSTALLATIONS

Ultimately, the only way we can guarantee that a component works, is if it is tested in the actual operating conditions. Lab-grade conformance and performance tests, only reveal so much. For this reason, it may be desirable to certify tagged objects and aggregations of tagged objects for supply chain use via actual interoperability tests. In such a test, a tagged object or aggregation of tagged objects should be registered by the tag applicator or primary user as intended for distribution in the supply-chain.

The applicator or user would submit a capability statement along with the tagged object or aggregation. The testing party, whether 1st, 2nd, or 3rd party, could match the intended applications against a broad cross section of registered reader installations. Tagged objects and/or aggregations could be tested in a small sample of reader installations. This would provide additional assurance that the component under test is interoperable.

3.2.5. Certification Program Management

As previously discussed, we can expect rapid change in the RFID industry. Technologies will improve and vendors will multiply. Applications will develop and users will multiply. At the same time, standards must closely follow (or lead). This applies to the certification program as well. In order to adapt most efficiently to change, the process itself, including the overall process as well as procedures for individual components should remain relatively steady. The actual standards and requirements, however, should be expected and designed to change. The appropriate management structure should be in place to handle this task. Input should be drawn from multiple users and vendors spanning industries and countries. The certified products and services registry should serve as a useful tool.

4. CONCLUSION AND NEXT STEPS

For the purpose of discussion, this paper has presented options and recommendations for a compliance and certification program for the Center. Though undoubtedly not the only requirement, such a program will be necessary in order to migrate from the current state of RFID implementation for closed systems towards RFID implementation in large open systems. In order to make this migration, all process and procedures should be designed around scale, flexibility, and coverage leading to a high degree of assurance of interoperability for the widest population of end users.

Process and procedures should be designed to scale to allow for improving capabilities of technology and new types, numbers, and locations of applications,

- Process and procedures should remain fixed, while the individual parameters can change.
- Test and evaluation methods should be repeatable, reliable, and reproducible allowing for global evaluation and use.

For evaluation, isolation of components is recommended wherever possible,

- Components control different parameters, frequencies, functionality, protocols and performance.
- Participants control different components.

Test coverage should be broad. Tests of isolated components should be supplemented with tests of systems. It is recommended to,

- perform conformance and performance tests with well-calibrated, well-known and widely used environments, equipment, and methods to isolate components and their attributes.
- perform interoperability tests of application specific systems to complement conformance and performance tests of isolated components.

Well-calibrated, well-known, and widely used environments and equipments should be used where possible. This should result in greater repeatability, reliability, and reproducibility. However, systems and protocols are multi-dimensional and complex. Simulation through existing test equipment and instrumentation can be costly.

- Special validated test tags and readers should be designed to automate testing and allow testing of full-operation rather than testing of individual parameters.

Simple standards on attributes such as frequency, protocols, functionality, and minimum levels of performance should be created wherever possible to improve clarity and ease adoption and implementation. At the very minimum, information regarding these attributes and options should be made available.

This can be achieved through:

- implementation conformance and intended application statements
- an accessible registry of information about certified components and systems
- supplementary guidelines

4.1. Next Steps

A great deal of work remains to be done in order to produce a functioning certification program. Process, documentation, testing , methods, and reporting methods will have to be discussed and developed. Test performers and program administrators will have to be identified.

- It is recommended that conformance and performance tests be developed by either independent experts or working groups consisting primarily of technology vendors and test experts, with input from users and oversight from the Center. In this way, tests can be designed to leverage, complement, and/or improve upon vendors existing efforts.

- Interoperability tests should be developed with input from both users and vendors. Interoperability tests are far more application and system centric.

- Process, documentation, reporting methods, management structures, and other policies – in particular who will perform tests (1st, 2nd or any of a number of 3rd parties) – should be developed by the Center with input from all relevant parties.

Facilities, equipment, and personnel will have to be identified and acquired. Much of this will be based on the Center's policies. However, development of calibrated and controllable test readers and tags should be considered.

Finally, research with the deliverable of implementation guidelines should be initiated.

6. REFERENCES

1. **Auto-ID Center, "860 MHz – 930 MHz Class 1 Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification, Candidate Recommendation, Version 1.0.0".**
   MIT-AUTOID-TR-007, Technical Report: November 14, 2002.

2. **Auto-ID Center, "Draft Protocol Specification for a 900 MHz Class 0 Radio Frequency Identification Tag".**
   February 23, 2002.

3. **Auto-ID Center, "13.56 MHz ISM Band Class 1 Radio Frequency Identification Tag Interface Specifiation, Candidate Recommendation, Version 1.0.0".**
   February 1, 2003

4. **T.A.Scharfeld, "An Analysis of the Fundamental Constraint on Low-Cost Passive Radio Frequency Identification System Design".**
   M.S. Thesis, Massachusetts Institute of Technology, Cambridge, MA, 2001.

5. **M. Reynolds, J. Richards, S. Pathare, H. Tsai, Y. Maguire, R. Post, R. Pappu & B. Schoner, "Multi-Band, Low-Cost EPC Tag Reader".**
   Auto-ID Center, Cambridge, MA, June 1, 2002.

6. **P. Cole, "A Study of Factors Affecting the Design of EPC Antennas & Readers for Supermarket Shelves".**
   Auto-ID Center, Adelaide, AU, June 1, 2002.

7. **ISO/IEC Guide 2.**
   1996.

8. **ISO, "Marks of Conformity Assessment".**
   1st ed., 1999.

9. **H.C.W. Gundlach, "Marks of Conformity for Production (Discussion Paper)".**
   European Organisation for Conformity Assessment, October 1999.

10. **ETSI, ETS 300406, "Methods for Testing and Specification (MTS); Protocol and Profile Conformance Testing Specifications; Standardization Methodology".**
    April 1995.

11. **P. O'Conner, "Test Engineering: A Concise Guide to Cost-effective Design, Development and Manufacture".**
    John Wiley & Sons, td, Chichester, UK, 2001.

12. **ANSI/IEEE Std 149-1979, "IEEE Standard Test Procedures for Antennas".**
    August 8, 1980.

13. **Bluetooth Qualification Program Website.**
    http://qualweb.bluetooth.org/Template2.cfm

14. **Bluetooth, "Specification Version 1.0 A: Compliance Requirements Part I:2".**
    Bluetooth SIG, July 24, 1999.

15. **BITE, "RF Tester Version 2.2".**
CETECOM S.A., Malaga, Spain, 2002.

16. **Qualification Program Reference Document.**
Bluetooth SIG, February 7, 2002.

17. **Test Specification: RF, Specification 1.1.**
Bluetooth SIG, February 1, 2002.

18. **N. Cravotta, "Bluetooth Interoperability: It's All in the Details".**
EDN, Reed Electronics Group, May 1, 2003.

19. **R. Schneiderman, "Bluetooth's slow dawn".**
IEEE Spectrum, Vol. 37, No. 11, November 2000.

20. **M. Gast, "802.11 "Standards Drift" and Interoperability Certification".**
O'Reilly Developer Weblogs, 2003 <http:/www/oreillynet.com/pub/wlg/2452>.

21. **WECA, "Wi-Fi System Interoperability Test Plan, Version 1.1a".**
December 11, 2001.

22. **S. Graves, "GSM Conformance Testing".**
http://www.compliance-club.com/archive1/020912.htm

23. **P. Albright, "Interoperability, Roaming Pushed At GSM Congress".**
Wireless Week, Reed Business Information, January 31, 2002.

24. **S. Eiland, "One Global Programme for Testing of Second and Third-generation Handsets".**
Business Briefing: Wireless Technology, 2002.

25. **GCF-PD, "Principles Document".**
Global Certification Forum, April 24, 2003.

26. **GSM Association, "GSM Certification Forum Program Overview".**
3GPP TSG SA, October 1999.

27. **CTIA Certification Program.**
http://www.wow-com.com/consumer/devices/certification/articles.cfm?ID=76

28. **CTIA, "Method of Measurement for Radiated RF Power and Receiver Performance, Revision 1.1".**
December 2001.

29. **B. Smith, "CTIA Boosts Handset Certification Program".**
Wireless Week, Reed Business Information, April 22, 2002.
IEEE Spectrum, Vol. 37, No. 11, November 2000.

30. **S. Sarma & D. Engels, "On the Future of RFID Tags and Protocols".**
Auto-ID Center, Cambridge, MA, June 17, 2003.

APPENDIX A: SUMMARY OF COMPONENTS AND THEIR CONTRIBUTIONS

Table 4

	CREATED BY	USED BY:	FREQUENCY INFLUENCE	PROTOCOL INFLUENCE	PERFORMANCE INFLUENCE – RANGE	PERFORMANCE INFLUENCE – SPEED	QUALITY/ VARIABILITY	# OPTIONS
TAGGED OBJECT								
CHIP	Chip Company, Tag Company	All	Major	Major – Logic – Memory	Major – Power rectification – Power consumption – Minor impedance mod.	Major – Via protocol – Via quality – Via Rx in noise	Variable	Few – Fixed
+ ANTENNA	Tag Company	All	Major	Minor – Matching factor	Major Power Rx/modulation (Tx) – Pattern, polarization, gain (UHF) – Area, # of turns (HF)	Via Range	Stable	Many – Size, shape, material
+ ATTACHMENT	Tag Company	All	Minor	Minor – Matching factor	Major/Minor – Loss	Via Range	Stable	Few
TAG	Tag Company	Packaging and All Users	See Chip, Antenna Attachment	Minor – Matching factor	Major	Via Range	Placement Variable	Many – Via antenna
+ OBJECT	Users	All Users	Minor	Minor – Matching factor	Major – Power reception – Power backscatter/load	Via Range	Stable	Many – Size, shape, materials, EM influence
TAGGED OBJECT	Packaging Company	All Users	Minor	Minor – Matching factor	Major – Placement of tag on object	Via Range	Placement Variable	Many – Via antenna & object
+ OTHER TAGGED OBJECTS		Some Users	Minor	Minor – Propagation	Major – Loss, shielding	Via Range	Placement Variable – Mixed pallet	Many – Via types & arrangement
AGGREGATION	Users	Some Users	Minor	Minor – Propagation	Major – Loss, shielding	Via Range	Placement Variable – Mixed pallet	Many – Via types & arrangement

Table 5

	CREATED BY	USED BY:	FREQUENCY INFLUENCE	PROTOCOL INFLUENCE	PERFORMANCE INFLUENCE – RANGE	PERFORMANCE INFLUENCE – SPEED	QUALITY/ VARIABILITY	# OPTIONS
READER INSTALLATION								
READER ELECTRONICS	Reader Company	Many Users – Fixed	Major – Primary	Major – Primary	Major – Power out via regulations	Major Algorithm – Rx sensitivity – Tx quality	Variable	Many – Frequencies – Protocols – Software/Hardware Radio – Performance – Network interface
+ ANTENNAS	Antenna Company, Reader Company	Many Users – Fixed	Major	Minor – Matching factor	Major Power Rx/Tx – Pattern, – Polarization, Gain (UHF) Area, # of turns (HF)	Via Range	Stable	Many Types Many Arrangments
+ CABLING	Cabling Company, Integrator	Many Users – Fixed	Minor	Minor – Matching factor	Major/Minor – Loss	Minor	Stable	Many types – Loss, Shielding factors – Variable lengths
+ FACILITY STRUCTURES, MACHINES, PEOPLE	User	Single User	Minor	Minor	Major – Shielding, loss	Minor – Via Range	Variable	Many
+ TEMPERATURE/ HUMIDITY	User	Single User	Minor	Minor	Major/Minor – Propagation (humidity)	Minor – – Matching – Stability (temp)	Variable – Unless controlled	Variable within and across facilities
+ EM NOISE	User	Single User	Minor	Minor	Minor – Jam tranmission	Major – Causes errors – Retransmission	Variable – Unless shielded	Variable within and across facilities
READER INSTALLATION	Integrator	Single User	See Reader & Antennas	See Above	See Above	See Above	See Above	See Above
USE	User	Single User	Minor	Minor	Major – Positions – Orientation tag relative to reader	Major – # of tags – Types of tags – Time in field – Noise from vibration	Variable – Unless automated & controlled	Many

APPENDIX B: SUMMARY OF OPTIONS AND RECOMMENDATIONS FOR COMPLIANCE TESTS

Table 6

COMPONENT	TEST TYPE	PURPOSE	SUBMIT DOCUMENTATION	SUBMIT DEVICE	TEST ENVIRONMENT	TEST EQUIPMENT	TEST PARAMETERS	REGISTER
CHIP	Conformance/ Performance	Isolate data, protocol & functionality controlled by chip.	Frequency, protocol & functionality	50 ohm coax I/O on PCB **OR,** Pre-validated reference antenna	Direct coax connection. **OR,** w/ref antenna: Anechoic chamber/ Open Field/Shielded box (protocol test only – not antenna)	Standard Instrumentation GPIB, Computer Control **OR,** Validated Test Reader w/test mode and API	Conformance: data, RF parameters (freq., timing, power), All Command primitives, operations Performance: sensitivities, modulation coefficient, power loss response	Frequency, protocol, functionality Key performance results
TAGS/TAGGED OBJECTS AND AGREGGATIONS	Conformance/ Performance	Check tags antenna/ attach for objects of three types: 1) Known type 2) Known class 3) Unknown	Chip type: Frequency, functionality and protocol, Intended objects (placement) Intended applications	Tag with object of known type, and class where appropriate.	Anechoic chamber/ Open field, or other validated environment	Standard instrumentation with positioners (turntable, stands), calibrated reference antennas **AND/OR** Validated Test Reader Test objects for unknown type.	If chip not tested, chip parameters, plus Gains, patterns polarizations (UHF), Pattern, orientation sensitivities (HF)	Submit document parameters, link to chip registration, plus key performance results
TAGGED OBJECTS AND AGREGGATIONS	Interoperability	Verify actual field operation	As above, Intended applications statement key	Tagged object and/ or aggregation	Actual registered reader installations	Validated test reader w/ existing antenna installation	Sample readability in broad cross section of registered reader installs **AND/OR** Actual reader install	Link to tagged object registration, intended (Pass/fail) applications
READERS	Conformance/ Performance	Isolate frequency, protocol, functionality, Tx/Rx, commands, algorithm	Frequencies, protocols and functionality, intended region of operation, intended antenna types	Reader w/ appropriate test hooks, test API	Direct coax connection	Std. inst. w/GPIB & computer control **AND/OR** Large population of validated test tags with API, OR actual calibrated tags, RF components for propagation sim.,	Conformance: Frequency, power, timing for protocols, functionality Performance: Read rate with varying tag population, simulated noise, prop. Loss, tag power loss	Supported frequencies, protocols, functionality, intended regions, antenna types, key performance parameters
ANTENNA (OPTIONAL) PERFORMANCE	Conformance/ Performance	For non-tested and integral antennas (i.e. handheld)	Reader characteristics as above	Intended Reader if integral	Anechoic chamber/ Open Field	Standard instrumentation with positioners for standard antenna measurement	Gain, pattern, polarization (UHF) Area, number of loops, etc. (HF)	Intended reader characteristics, Tested parameters
READER INSTALLATIONS	Registration/ Conformance/ Performance	Verify reader install, environmental factors, register applications	Statement of components in installation technology and application	Existing field implementation	Actual conditions (Field test/inspection)	Test instrumentation (spectrum analyzer) AND/OR test tags with calibrated antenna/probe	Environmental noise, temperature/ humidity, Field strength levels	Application type, environmental characteristics, supported component options
READER INSTALLATIONS	Interoperability	Verify actual field operation	As above	As above	As above	Actual tagged objects, different tag types	Sample readability of cross-section of registered/expect tagged objects – tag types, object types	Application type, supported component options

Designed by Foxner. www.foxner.com