Discovery, Configuration, and Initialization (DCI)

for Reader Operations

Version: Ratified Standard 1.0

June 10, 2009

Disclaimer

EPCglobal Inc™ is providing this document as a service to interested industries. This document was developed through a consensus process of interested parties. Although efforts have been to assure that the document is correct, reliable, and technically accurate, EPCglobal Inc. makes NO WARRANTY, EXPRESS OR IMPLIED, THAT THIS DOCUMENT IS CORRECT, WILL NOT REQUIRE MODIFICATION AS EXPERIENCE AND TECHNOLOGICAL ADVANCES DICTATE, OR WILL BE SUITABLE FOR ANY PURPOSE OR WORKABLE IN ANY APPLICATION, OR OTHERWISE. Use of this document is with the understanding that EPCglobal Inc has no liability for any claim to the contrary, or for any damage or loss of any kind or nature.

Please be advised that this DCI Standard references the CAPWAP protocol from IETF. As always your legal counsel should review the standard and protocol for intellectual property issues before implementation.

Abstract

This document specifies a new device, called an Access Controller, which performs several DCI functions. This document also specifies several initial configuration requirements that an RFID Reader or Client must satisfy, in order for DCI operations to be successful. The purpose of the protocol specified here is to identify how the Reader is able to discover one or more Clients, the Client to discover one or more Readers, and for the Reader to obtain configuration information, download firmware, and initialize operations to allow other Reader Operation protocols to operate.

Audience for this document

The target audience for this specification includes:

RFID Network Infrastructure vendors

Reader vendors

EPC Middleware vendors

System integrators

Status of this document

This section describes the status of this document at the time of its publication within the Working Group, Technical and Business Steering Committees and the EPCglobal Board. This document has completed all the required EPCglobal Standards Development Process steps and it has been fully ratified by the EPCglobal Board on June 10th, 2009.

Comments on this document should be sent to the attention of EPCglobal Software Action Group Reader Operations Working Group using the following email address: epcinchelp@epcglobalinc.org.

Table of Contents

1 Introduction

This document specifies an interface between RFID Readers and Access Controllers and the network on which they operate. The purpose of this document is to specify the necessary and optional operations of a Reader and Client that allow them to utilize the network to which they are connected to communicate with other devices, exchange configuration information, and initialize the operation of each Reader, so that the Reader Operations Protocols can be used to control the operation of the Readers to provide tag and other information to the Client. To facilitate these operations by the Reader, an Access Controller provides several functions, described below.

Following are the responsibilities of this interface:

- Provide a means for the Reader to discover one or more Access Controllers.
- Provide a means for the Access Controller to discover one or more Readers.
- Provide a means for the Reader to discover one or more Clients.
- Provide a means for the Reader and Access Controller to exchange identity information and authenticate that identity information.
- Provide a means for the Client and Access Controller to authenticate their communications and operations.
- Provide a means for the Access Controller to configure the Reader, including a means to update the software and/or firmware on the Reader.
- Provide a means for the Access Controller to initialize the Reader, providing parameters necessary for the Reader to begin operation.
- Provide a means for the Reader and Access Controller to exchange vendor-specific information.

The Access Controller is a function that is described in this specification to separate these functions from those of a Reader or Client. An Access Controller can be coincident with a host running other Reader Operations protocols or it can be in a separate host. The following figure shows the relationships between the Reader, Client, other network services, and Access Controller.

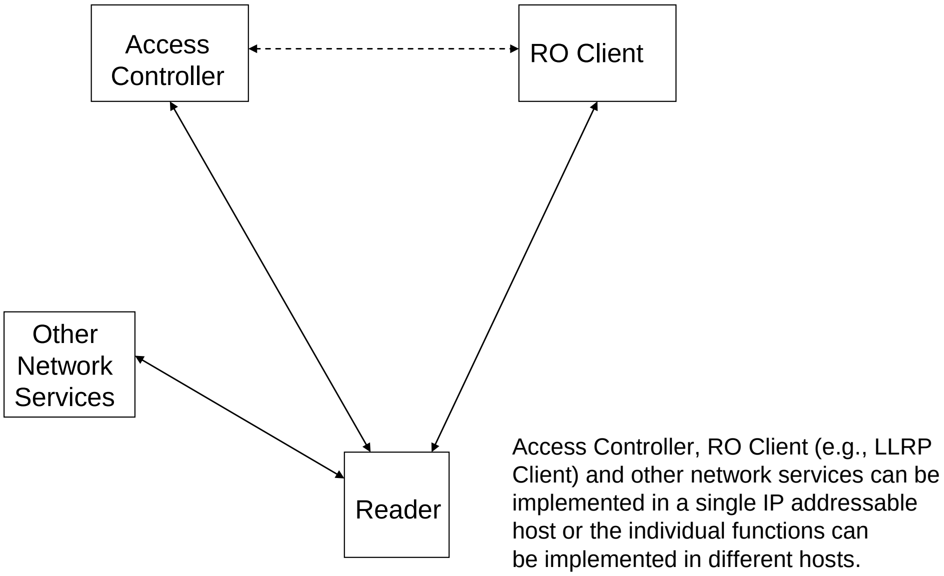

Access Controller
RO Client
Other Network Services
Reader
Access Controller, RO Client (e.g., LLRP Client) and other network services can be implemented in a single IP addressable host or the individual functions can be implemented in different hosts.

Figure 1-1, DCI network architecture

2 Role within the EPCglobal Network Architecture

Within the EPCglobal architecture, DCI performs a Reader Management (RM) role, but addresses different requirements than the existing Reader Management specification **[RM]**. DCI and RM do not depend on each other, so products can choose to implement either, neither, or both of RM and DCI. Specifically, the EPCglobal RM specification defines methods for monitoring the health of Readers and allowing readers to notify management systems of potential issues. The DCI specification provides requirements and protocols that are implemented in both the Reader and an Access Controller device, allowing each to discover the other on the network, allowing the Access Controller to configure the Reader, to download firmware to the Reader, and to initialize the operation of the Reader. The access control function is not described in the current EPCglobal architecture.

3 Terminology and Typographical Conventions

Within this specification, the terms SHALL, SHALL NOT, SHOULD, SHOULD NOT, MAY, NEED NOT, CAN, and CANNOT are to be interpreted as specified in Annex G of the ISO/IEC Directives, Part 2, 2001, 4th edition **[ISODir2]**. When used in this way, these terms will always be shown in ALL CAPS; when these words appear in ordinary typeface they are intended to have their ordinary English meaning. However in this document only a subset of the terms listed above SHALL be used. The subset of acceptable terms includes the following: SHALL and MAY. The terms, SHOULD, SHOULD NOT, NEED NOT, CAN, and CANNOT, SHALL NOT be used.

All sections of this document, with the exception of Section 1 and Section 2, are normative, except where explicitly noted as non-normative.

The following typographical conventions are used throughout the document:

ALL CAPS type is used for the special terms from [ISODir2] enumerated above.

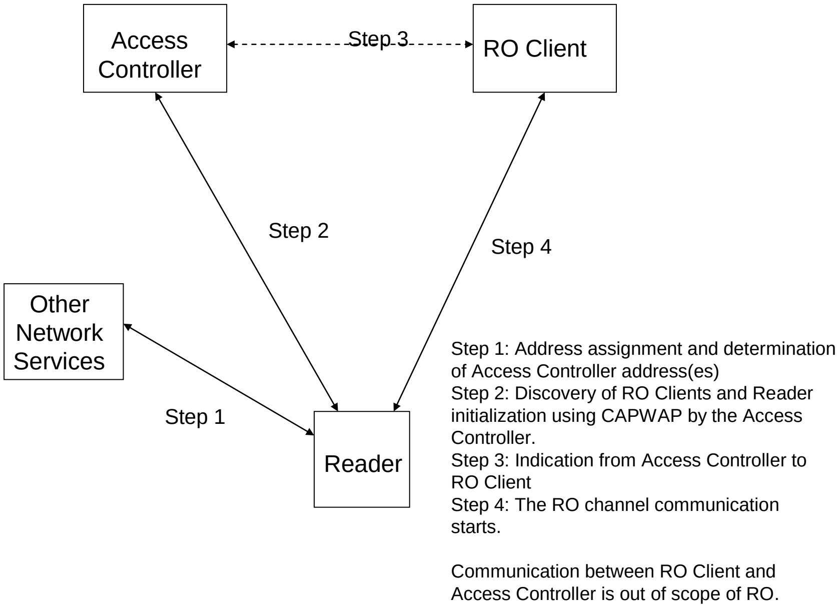
`Monospace` type is used to denote programming language, UML, and XML identifiers, as well as for the text of XML documents.

4 Overview of DCI

DCI provides a Reader with the information necessary to establish or accept a connection with a Client across a network. DCI provides initial device configuration to a Reader, sufficient to begin network communication. DCI also provides firmware image management for a Reader.

DCI utilizes the Control and Provisioning of Wireless Access Points (CAPWAP) protocol **[CAPWAP]**. CAPWAP must be implemented by both the Reader and the Access Controller. DCI operation comprises the following phases:

- Device discovery
- Device authentication and identity exchange
- Firmware download, if necessary
- Device configuration
- Device initialization



Step 1: Address assignment and determination of Access Controller address(es)
Step 2: Discovery of RO Clients and Reader initialization using CAPWAP by the Access Controller.
Step 3: Indication from Access Controller to RO Client
Step 4: The RO channel communication starts.

Communication between RO Client and Access Controller is out of scope of RO.

Figure 4-1, DCI Overview

5 Initial Conditions for Reader and Access Controller

In order for a Reader and Access Controller to communicate on a network, a proper IP address must be used by each device. It is the responsibility of the manufacturer to provide a means for the Reader or Access Controller device to obtain an IP address and other such IP configuration information necessary to operate on the network to which the device is attached. It is beyond the scope of this document to specify how this information is obtained. It is also the responsibility of the Reader manufacturer to provide a means for the Reader to obtain the IP address of at least one Access Controller and for the Access Controller manufacturer to provide a means for the Access Controller to obtain the IP address of at least one Reader. There are several methods that might be used to obtain the IP addresses of a Reader or Access Controller. Specification of these methods is beyond the scope of this document.

6 Discovery protocol

Using an IP address of an Access Controller device, the Reader exchanges messages with the Access Controller, identifying and authenticating itself to the Access Controller device.

6.1 Discovery protocol operation

The Reader and Access Controller device SHALL implement the discovery protocol as described in the CAPWAP protocol **[CAPWAP]**. The Reader device SHALL perform as a wireless termination point (WTP), as described in **[CAPWAP]**. The Access Controller device SHALL perform as an access controller (AC) as described in **[CAPWAP]**. Both the WTP and AC SHALL implement the complete CAPWAP protocol, to the extent that any legal CAPWAP frame received is processed as required in **[CAPWAP]** and a valid response is transmitted when required by the protocol. Should the WTP or AC receive a CAPWAP packet or a message element in a CAPWAP packet that is optional or that is not understood by the implementation, the minimum behavior required of the implementation is that the unknown material is gracefully ignored and any required CAPWAP response is properly transmitted.

6.2 Reader operation during discovery

The Reader shall begin the discovery process by sending a CAPWAP Discovery Request message to one or more Access Controller addresses determined by manual, DNS, DHCP configuration, or broadcast. If the Reader is configured with a Primary Access Controller, analogous to the Primary AC in **[CAPWAP]**, the Reader shall send the CAPWAP Discovery Request message. The format of the Discovery Request or Primary Discovery Request message shall be as defined in section 5.1 or 5.3 of **[CAPWAP]**, respectively. The content of the individual message elements contained in the Discovery Request shall be as defined below.

6.2.1 Discovery Type

The value of the Discovery Type field shall indicate the method used to obtain the address of the Access Controller that is addressed by the Discovery Request message.

6.2.2 WTP Descriptor

The fields of the WTP Descriptor shall contain the information described in 4.6.41 of **[CAPWAP]**. The value of the Active Software Version field contained within the WTP Descriptor SHALL be encoded with the same format as the value encoded in the Image Identifier such that upon downloading an image referenced by an Image Identifier and activating that image through reboot, the WTP reports as the value in its new Active Software Version field the same image identifier value. The value of the Other Software Version field contained within the WTP Descriptor SHALL be encoded with the same format as the Active Software Version field.

6.2.3 WTP Frame Tunnel Mode

The value of the Tunnel Mode field of the WTP Frame Tunnel Mode message element shall be 1, indicating local bridging. This field is required for compliance with CAPWAP. It has no significance for DCI. The format of this field is described in 4.6.43

of **[CAPWAP]**.

6.2.4 WTP MAC Type

The value of the MAC Type field of the WTP MAC Type message element shall be 0, indicating Local MAC. This field is required for compliance with CAPWAP. It has no significance for DCI. The format of this field is described in 4.6.46 of **[CAPWAP]**.

6.3 Access Controller operation during discovery

The Access Controller shall respond to all Discovery Request and Primary Discovery Request messages with a Discovery Response or Primary Discovery Response message, as described in section 5.2 and 5.4 of **[CAPWAP]**, respectively. The content of both messages is defined below.

6.3.1 AC Descriptor

The fields of the AC Descriptor message element shall be set as follows.

The Stations field shall be 0. This field is required for compliance with CAPWAP. It has no significance for DCI.

The Limit field shall be 0. This field is required for compliance with CAPWAP. It has no significance for DCI.

The Active WTPs field shall indicate the number of Readers currently joined to the Access Controller.

The Max WTPs field shall indicate the maximum number of Readers that the Access Controller is able to support.

The Security field shall indicate the credential used by the AC, as defined in section 4.6.1 of **[CAPWAP]**.

The R-MAC and Wireless fields shall be 0. This field is required for compliance with CAPWAP. It has no significance for DCI.

The remaining fields shall contain values as specified in section 4.6.1 of **[CAPWAP]**.

6.3.2 AC Name

The Name field of the AC Name message element shall contain a UTF-8 string, as defined in 4.6.4 of **[CAPWAP]**.

6.3.3 CAPWAP Control IPv4 Address

Both the IP Address and WTP Count fields of this message element shall be 0. This field is required for compliance with CAPWAP. It has no significance for DCI.

6.3.4 CAPWAP Control IPV6 Address

Both the IP Address and WTP Count fields of this message element shall be 0. This field is required for compliance with CAPWAP. It has no significance for DCI.

7 Device identification and authentication

The Reader and Access Controller devices SHALL use DTLS **[DTLS]** to perform the necessary exchange of identity and authentication, as described in **[CAPWAP]**. Upon successful establishment of the DTLS tunnel, the Reader and Access Controller devices SHALL perform the Join portion of the CAPWAP protocol, as described in **[CAPWAP]**.

8 Firmware download

Once the Reader and Access Controller devices have completed the Join portion of the CAPWAP protocol, the Reader has provided the Access Controller with its firmware version information. The Access Controller may implicitly trigger the start of the download by the WTP by sending an image information different than the age currently active on the Reader. The Access Controller and Reader SHALL support the firmware download mechanism described in section 9.1 of **[CAPWAP]**. It should be noted that, while the operation is called “firmware download”, this mechanism allows the download of arbitrary files, identified by their file desctriptor (it could be name, version number, etc) (see section 8.1.2).

When operating in the CAPWAP Run state, an AC MAY indicate any file in an Image Identifier. The Reader SHALL commence downloading the image, when the file indicated by the Image Identifier does not match the corresponding local file, even if the local file does not exist. If the image downloaded corresponds to a firmware or software file, the Reader SHALL begin executing the image upon the next hardware or software reset event. If the image downloaded does not correspond to a firmware or software file, DCI makes no requirements on how such a file is handled.

When operating in the CAPWAP Join state, an AC SHALL indicate only a file corresponding to a firmware or software file in the Image Identifier of the Join Response packet. If the Reader receives an Image Identifier other than one corresponding to a firmware or software file, the Reader SHALL ignore the Image Identifier. After successfully downloading an image in the CAPWAP Image Date state, the Reader SHALL reset and begin executing the newly downloaded image immediately.

8.1 Access Controller operation during download

The Access Controller shall use the Image Data Request message, as described in section 9.1.1 of **[CAPWAP]**. The content of the Image Data Request message shall be as described below.

8.1.1 Image Data

The content of this message element shall be as described in section 4.6.27 of **[CAPWAP]**.

8.1.2 Image Identifier

This message element shall be sent to the Reader by the Access Controller to begin the download process. The content of the Value field shall be as described in 4.6.28 of **[CAPWAP]**. The value of the Active Software Version field contained within the WTP Descriptor SHALL be encoded with the same format as the value encoded in the Image Identifier, such that upon downloading an image referenced by an Image Identifier and activating that image through reboot, the WTP reports as the value in its new Active Software Version field the same image identifier value. Similarly, the Other Software Version field contained within the WTP Descriptor SHALL be encoded with the same format as the Active Software Version field.

8.2 Reader operation during download

The Reader shall respond to each Image Data Request message with an Image Data Response message, as described in section 9.1.2 of **[CAPWAP]**.

9 Reader Device Configuration

Using **[CAPWAP]** control frames, the Reader device SHALL inform the Access Controller of its current configuration. The Access Controller device SHALL use **[CAPWAP]** control frames to make any changes to the Reader device configuration, including providing the Reader with the information necessary for it to communicate with Clients providing Reader Operations protocols.

9.1 Configuration Status message

The Reader SHALL send the Configuration Status message to the AC, as described in section 8.2 of **[CAPWAP]**. The message element that has values specified in DCI is:

9.1.1 Radio Administrative State

The Radio Administrative State message element SHALL contain the Radio ID and Admin State as defined in 4.6.31 of **[CAPWAP]**. The values for these fields SHALL be zero when sent by the WTP and ignored by the AC on reception. This element SHALL NOT be used for managing the radio(s) in the WTP. Radio management is the responsibility of the reader protocol.

9.2 Configuration Status Response message

The AC SHALL send the Configuration Status Response message to the Reader, as described in section 8.3 of **[CAPWAP]**.

9.3 Configuration Update Request message

The AC SHALL send the Configuration Update Request message to the Reader, as described section 8.4 of **[CAPWAP]**. In addition to the message elements listed in **[CAPWAP]**, the AC MAY send one or more Client message elements (see 9.5.3) or Reader Configuration message elements (see 9.5.4). The AC MAY send a single Reader Role message element. As described in 9.1.3, the Radio Administrative State message element SHALL NOT be used for managing the radio(s) in the WTP. Radio management is the responsibility of the reader protocol.

9.4 Configuration Update Response message

In response to the receipt of a Configuration Update Request message, the Reader SHALL send a Configuration Update Response message, as described in section 8.5 of **[CAPWAP]**.

9.5 EPCglobal binding-specific CAPWAP message elements

This section defines the EPCglobal binding specific CAPWAP protocol message elements. As specified in CAPWAP, each message element uses the TLV (Type, Length, Value) format. The CAPWAP protocol has allocated type values 3072-4095 for EPGglobal message elements (Section 4.6 of [CAPWAP]). Because that number space is intended to be used for RFID-related message element requirements, this specification further divides the EPCglobal number space to allow other RFID standards bodies such as ISO to extend the DCI protocol with message elements specific to their requirements. To that effect, the EPCglobal type value space is further segmented as:

EPCglobal Message Elements	3072-3899
ISO Message Elements	3900-3994
RFU	3995-4095

9.5.1 EPCglobal Radio Information

This is a null message element. The format of the message element is shown in Figure 9-1.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              Type             |             Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 9-1, EPCglobal Radio Information message element

Type: The value of the Type filed SHALL be 3072 (decimal).

Length: The value of the Length field SHALL be zero.

9.5.2 EPCglobal Statistics message element

The definition of this message element is required for compliance with the CAPWAP protocol. This is a null message element. All statistics information is carried in other EPCglobal protocols. The format of the message element is shown in Figure 9-2.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              Type             |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 9-2, EPCglobal Statistics message element

Type: The value of the Type filed SHALL be 3073 (decimal).

Length: The value of the Length field SHALL be zero.

9.5.3 Client message element

The Client message element is a binding specific message element and SHALL conform to the format for such message elements defined in section 4.6 of **[CAPWAP]**. The Client message element provides information to the Reader about a single Client device. The format of the message element is shown Figure 9-3.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              Type             |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           IP Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Port Number         |I|A|T|        Protocol         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Credentials                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 9-3, Client message element

Type: The value for the Type field shall be 3074 (decimal).

Length: The value of the Length field shall be 12 (decimal).

IP Address: The IP Address is the address of the host containing the Client.

Port Number: The Port Number is the port at which to contact the Client to open a connection.

I: The I flag indicates that the Client supports the Reader performing in the initiator role when contacting the Client.

A: The A flag indicates that the Client supports the Reader performing in the Acceptor role.

T: The T flag indicates that the Client requires the protocol session to be protected using TLS.

Protocol: This field identifies the reader protocol using the indicated Port Number. The field is a 13-bit integer. The values for each supported protocol are given in Table 9-1.

Value	Protocol
0	LLRP 1.x
1-8191	Reserved for future standardization

Table 9-1, Protocol Values

Credentials: The Credentials field is a bit field indicating the credential types supported by the reader protocol Client for establishment of a TLS session. This field SHALL be transmitted as zero when the T flag is zero. This field SHALL be ignored on receipt when the T flag is zero. The supported credentials are shown in Table 9-2.

Bit	Credential Type
0	X.509 Certificate
1-31	Reserved

Table 9-2, Credential Types

9.5.4 Reader Configuration message element

The Reader Configuration message element provides information to the Reader on the configuration it is to adopt. The format of the message element is in Figure 9-4.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              Type             |             Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|C|                         Reserved                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 9-4, Reader Configuration Message Element

Type: The value for the Type field shall be 3075 (decimal).

Length: The value of the Length field shall be 4 (decimal).

C bit: The C bit is used to indicate that the Reader is allowed to accept or establish connections using reader protocols independent of the CAPWAP state machine, when the value of the bit is 1. When the value of the bit is zero, the Reader is allowed to accept or establish connections using reader protocols only when the CAPWAP state machine is in the RUN state (see section 2.3 of **[CAPWAP]**.

9.5.5 Reader Role message element

The Reader Role message element provides a means to initialize the value for the role of the reader. The format of the message element is in Figure 9-5.

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |              Type             |             Length            |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                             Role                              |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 9-5, Reader Role Message Element

Type: The value for the Type field shall be 3076 (decimal).

Length: The value of the Length field shall be equal to the length of the Role field plus 4.

Role: The Role field is a UTF-8 string. The string is NOT zero terminated.

10 Connections

This section describes the requirements for the CAPWAP and other protocols the Reader implements with regard to those protocol connections.

10.1 CAPWAP connection

After completing CAPWAP discovery, the Reader and Access Controller SHALL maintain the CAPWAP connection using the CAPWAP Echo and Echo Response packets, as described in section 7 of **[CAPWAP]**. The Reader SHALL perform in the role of the CAPWAP WTP. The Access Controller SHALL perform in the role of the CAPWAP AC. Both Reader and Access Controller SHALL implement the CAPWAP Timers message element defined in section 4.6.14 of **[CAPWAP]**.

10.2 Other reader protocol connections and migration scenario

It is expected that Readers will be deployed prior to the completion of the DCI protocol and the availability of Access Controllers. This will lead eventually to deployments where there are Readers that do not implement DCI with Readers that do implement DCI on the same network. It is desirable to be able to deploy the Readers that do implement DCI in the same fashion as those already in the network that do not implement DCI. This requires that the DCI-capable Reader be able to operate with DCI disabled, as well as with DCI enabled.

In order to support network configurations where Readers have been deployed prior to the availability of certification of the DCI protocol, a Reader SHALL have a mechanism to configure when the Reader is allowed to establish a connection using another reader protocol, e.g., LLRP. This mechanism SHALL provide the following configurations, at a minimum.

1. The Reader can establish or accept a connection using another reader protocol at any time.

2. The Reader can establish or accept a connection using another reader protocol only after successful completion of DCI, i.e., the CAPWAP protocol state machine is in the Run state (see section 2.3 of **[CAPWAP]**).

11 Reader reset operation

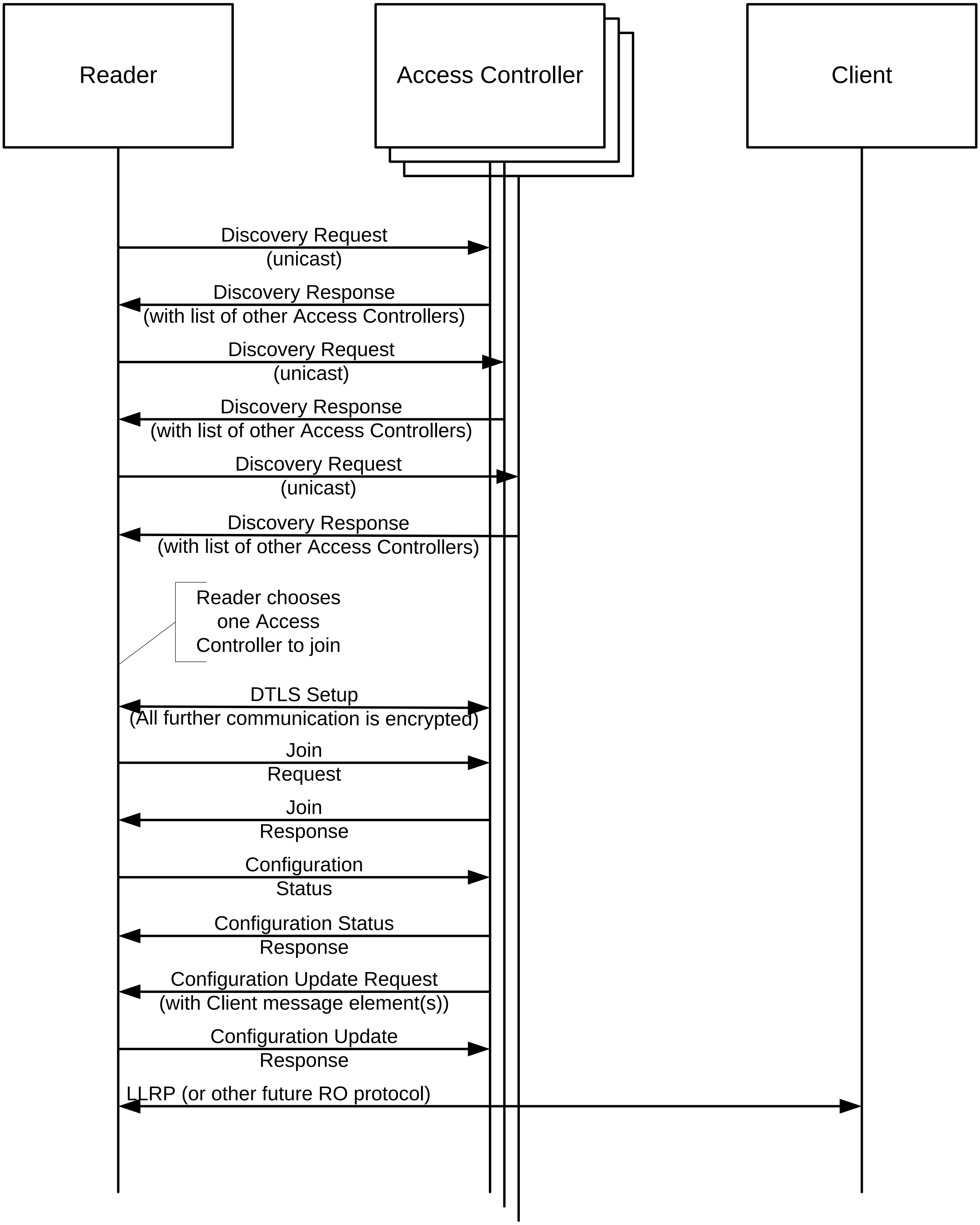
After the download of a new firmware image or at other times determined by the Access Controller, the Reader will be reset. To reset the Reader, the Access Controller SHALL send a CAPWAP Reset Request packet to the Reader. Upon receipt of the Reset Request packet, the Reader SHALL respond with a CAPWAP Reset Response packet.

12 (Informative) Message sequence charts

This section presents several message sequence charts to help understand the protocol operation.

Once the Reader has an IP address of its own, the Reader can proceed to use the CAPWAP protocol to discover Access Controllers and to join with one of them. After joining an Access Controller, the Reader is provided with the information necessary to communicate with an LLRP (or other future reader protocol) Client. This is shown in Figure 12-1.

459


Reader
Access Controller
Client
Discovery Request (unicast)
Discovery Response (with list of other Access Controllers)
Discovery Request (unicast)
Discovery Response (with list of other Access Controllers)
Discovery Request (unicast)
Discovery Response (with list of other Access Controllers)
Reader chooses one Access Controller to join
DTLS Setup (All further communication is encrypted)
Join Request
Join Response
Configuration Status
Configuration Status Response
Configuration Update Request (with Client message element(s))
Configuration Update Response
LLRP (or other future RO protocol)

460 n

Figure 12-1, Unicast Discovery Operation

When the Reader and Access Controller are on the same IP subnet, CAPWAP provides a broadcast discovery mechanism. This is shown in Figure 12-2.

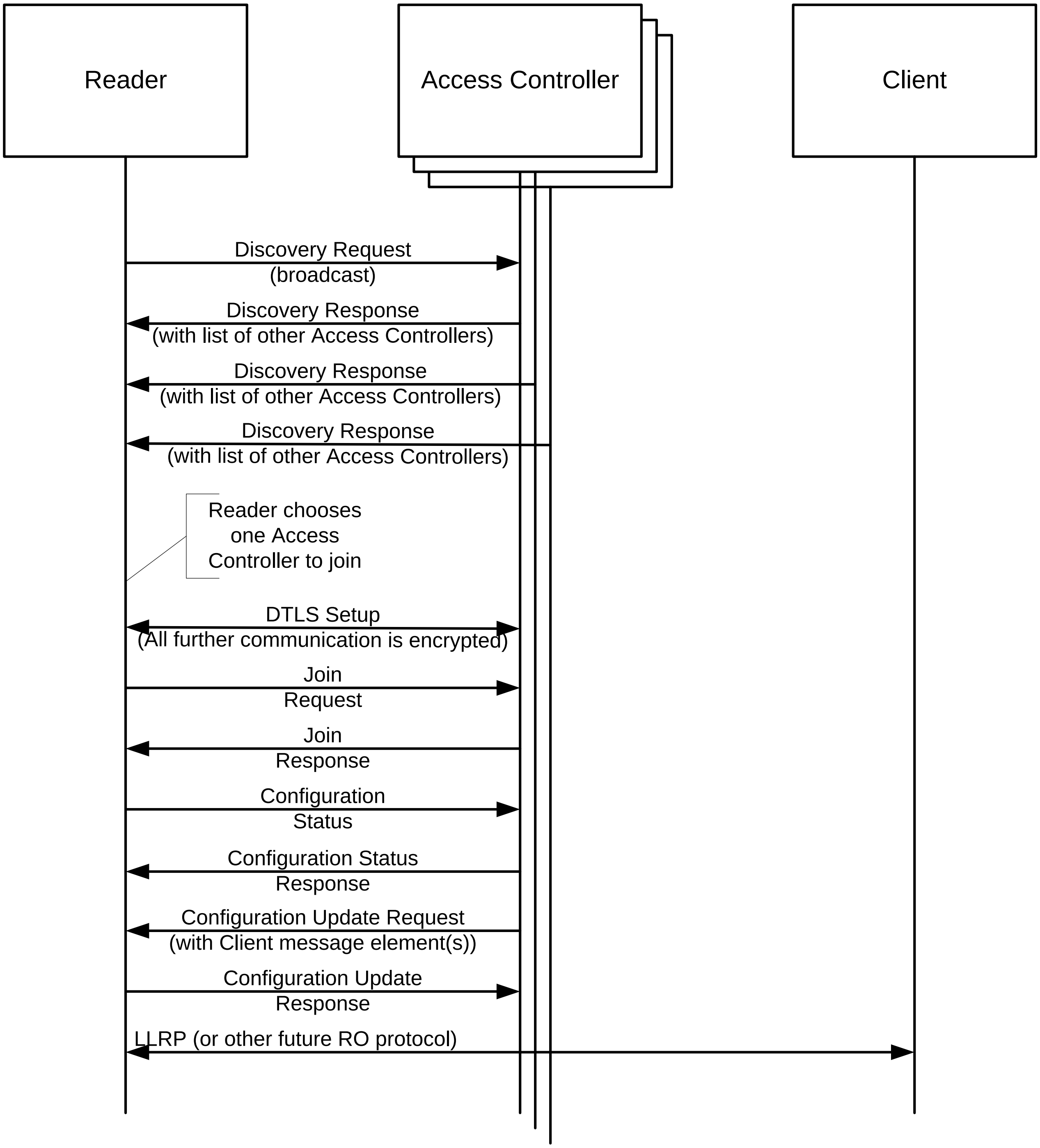

Reader
Access Controller
Client
Discovery Request (broadcast)
Discovery Response (with list of other Access Controllers)
Discovery Response (with list of other Access Controllers)
Discovery Response (with list of other Access Controllers)
Reader chooses one Access Controller to join
DTLS Setup (All further communication is encrypted)
Join Request
Join Response
Configuration Status
Configuration Status Response
Configuration Update Request (with Client message element(s))
Configuration Update Response
LLRP (or other future RO protocol)

Figure 12-2, Broadcast Discovery Operation

Once a Reader has joined an Access Controller, the Access Controller can download firmware updates to the Reader. The Access Controller can also cause the Reader to reset and begin operation using the new firmware. This operation is shown in Figure 12-3.

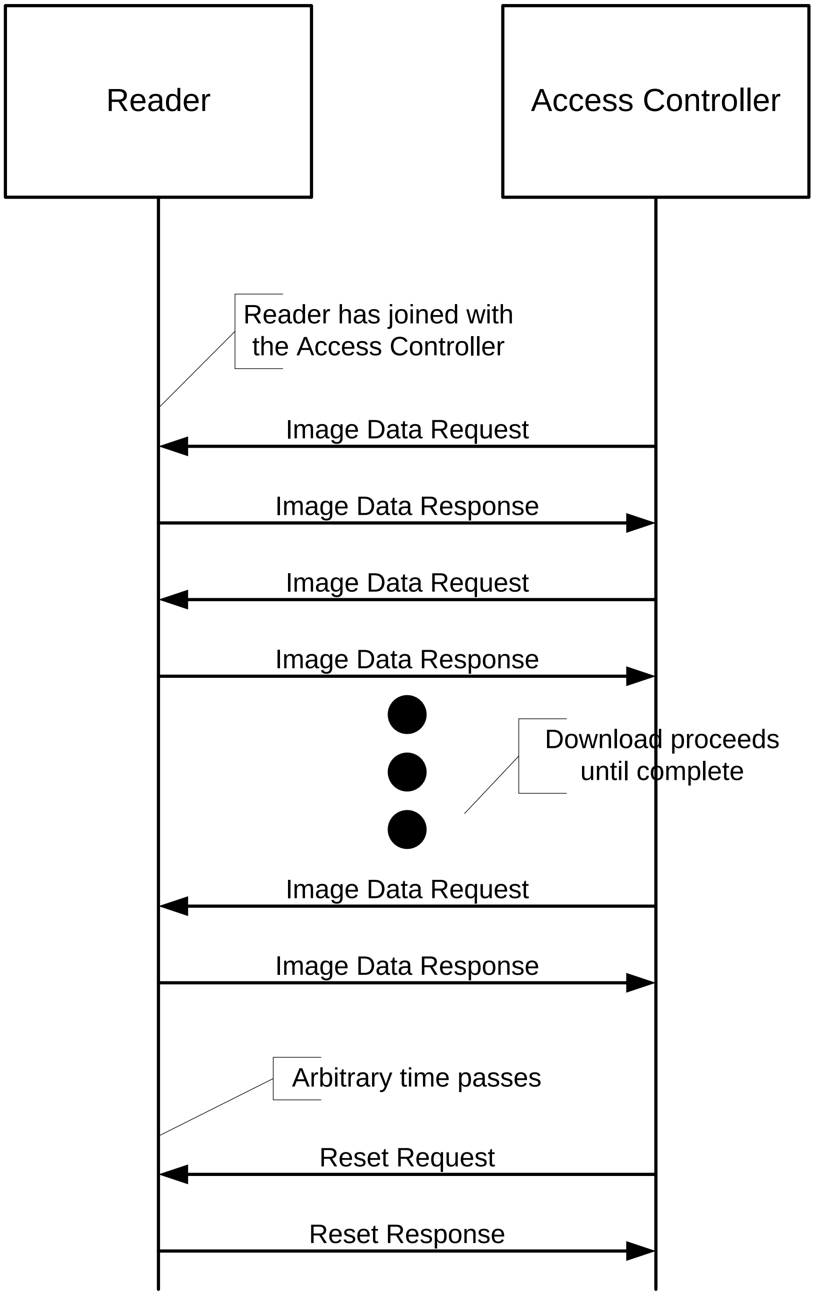


Figure 12-3, Firmware Download Operation

13 (Informative) Glossary

This section provides a non-normative summary of terms used within this specification.

Term	Meaning

14 Normative References

[ISODir2] ISO, “Rules for the structure and drafting of International Standards (ISO/IEC Directives, Part 2, 2001, 4th edition),” July 2002.

[ARC] EPCglobal Architecture Framework 1.3,

http://www.epcglobalinc.org/standards/architecture/architecture_1_3-framework-20090319.pdf

[RM] EPCglobal Reader Management Standard v1.0.1, http://www.epcglobalinc.org/standards/rm/RM_1_0_1-StandardRatified-20070531.pdf

[DHCP] rfc1531 - Dynamic host control protocol, http://www.ietf.org/rfc/rfc1531.txt

[DNS] rfc1035 - Domain names - implementation and specification, http://www.ietf.org/rfc/rfc1035.txt

[CAPWAP] rfc5415 Control and Provisioning of Wireless Access Points (CAPWAP) , http://www.rfc-editor.org/rfc/rfc5415.txt

[DTLS] rfc4347 - Datagram Transport Layer Security, http://www.ietf.org/rfc/rfc4347.txt

15 Acknowledgement of Contributors and Companies Opt’d-in during the Creation of this Standard (Informative)

Disclaimer

Whilst every effort has been made to ensure that this document and the information contained herein are correct, EPCglobal and any other party involved in the creation of the document hereby state that the document is provided on an “as is” basis without warranty, either expressed or implied, including but not limited to any warranty that the use of the information herein with not infringe any rights, of accuracy or fitness for purpose, and hereby disclaim any liability, direct or indirect, for damages or loss relating to the use of the document.

Below is a list of more active participants and contributors in the development of DCI 1.0. This list does not acknowledge those who only monitored the process or those who chose not to have their name listed here. Active participants status was granted to those who generated emails, attended face-to-face meetings and conference calls that were associated with the development of this Standard.

First Name	Last Name	Company	Notable Role
Dave	Husak	Reva Systems	Co-Chair
Rob	Buck	Intermec	Co-Chair
Pattabhiraman	Krishna	Reva Systems	Editor
Mark	Frey	EPCglobal Inc.	Facilitator for WG
Software Team at Impinj		Impinj	Minutes Recorder
Marc	Horowitz	BEA Systems	
Suresh	Bhaskaran	Intelleflex	
Daniel	Paley	Tagent Corp.	
Bud	Biswas	Polaris Networks	
Bob	O'Hara	Cisco	
Daniel	Bowman	Kimberly-Clark Corp	
Margaret	Wasserman	ThingMagic, LLC	
Arthur	Howarth	Cisco	
Richard	Bach	GlobeRanger	
Rick	Schuessler	Symbol Tech./Motorola	
Howard	Kapustein	Manhattan Associates	
David	Missimer	Sirit	
Darrel	Pinson	Symbol Technologies, Inc.	
Matt	Poduska	Intermec	
Steve	Lockhart	Sirit	
David	Lavin	IBM	
Lynn	Hingst	Intermec	
John	Walter	Intermec	
Soumya	Roy chowdhury	Polaris Networks	
Martin	Jackson	Wal-Mart	
Steve	Lin	Sirit	
Bryan	Tracey	GlobeRanger	
Scott	de Deug	IBM	
Ted	Osinski	MET Labs	
Scott	Barvick	Reva Systems	
Manpreet	Singh	Symbol Technologies, Inc.	
Heena	Nandu	Intelleflex	

Gerhard	Gangl	7iD (formerly EOSS GmbH)	
Bill	Bares	Intelleflex	
Jim	Sykes	Savi Networks	
Sudhir	Hasbe	Sirit	
Albert	Lin	WJ Co.	
Shigeya	Suzuki	Auto-ID Labs - Japan	
Gay	Whitney	EPCglobal Inc.	
Jim	Reed	MET Labs	
Matthew	Harmon	Q.E.D. Systems	
Ricardo	Labiaga	Sun Microsystems	
Mark	Richardson	ThingMagic, LLC	
David	Nesbitt	Vue Technology	
Roger	Stewart	Applied Wireless (AWID)	
Yukiko	Yumoto	Auto Id Lab Japan	
Abel	Sanchez	Auto-ID Labs - MIT	
John	Williams	Auto-ID Labs - MIT	
Mark	Sompel	AWID	
Ken	Traub	BEA Systems	
Matt	Robshaw	France Telecom	
Wayne	Liu	Impinj	
Tareef	Al-Mahdawi	Intelleflex	
Joe	Kubler	Intermec	
John	Walter	Intermec	
Peter	Anderla	KCC	
John	Boulas	KCC	
John	Anderla	KCC	
Moon Suk	Kim	Metarights	
Chang Yeol	Lee	Metarights	
Jens	Kungl	Metro	
Isao	Kimata	NEC Corporation	
Satoshi	Kinoshita	NEC Corporation	
Hiroki	Tagato	NEC Corporation	
Sergio	Lobo	NXP Semiconductors	
Gregory	Grisco	Oracle Corporation	

Jahangir	Nakra	Procter & Gamble	
Trong	Le	Psion Teklogix Inc.	
Craig	Harmon	Q.E.D. Systems	
Peter	Spreadborough	Reva Systems	
Sudhir	Hasbe	Samsys	
Steve	Winkler	SAP	
Sengu	Elango	Savi	
Neal	Herman	Savi	
Don	Ahn	Savi Technology	
L. Julia	Zhu	Savi Technology	
Pankaj	Shukla	Symbol	
Jong	Park	Tibco	
Keith	Rider	Tyco / ADT	
Bob	Sawdye	Tyco / ADT	
David	Harty	VeriSign	
Richard	Campero	Vue Technology	

The following list in corporate alphabetical order contains all companies that were opt'd-in to the Reader Operations Working Group and have signed the EPCglobal IP Policy.

Company
(ETRI) Electronics and Telecommunications Research Institute
7iD (formerly EOSS GmbH)
Accenture
Acer Cybercenter Service Inc.
Altria Group, Inc./Kraft Foods
Applied Wireless (AWID)
Ark Tech Ltd
Auto-ID Labs - Cambridge
Auto-ID Labs - Japan
Auto-ID Labs - MIT
BEA Systems
Blackbay Ltd.

CAEN
Cisco
Convergence Sys Ltd
Dai Nippon Printing
Denso Wave Inc
ECO, Inc.
EPCglobal Inc.
FEIG Electronic
France Telecom
Fujitsu Ltd
GlobeRanger
GS1 Australia EAN
GS1 Germany (CCG)
GS1 Hong Kong
GS1 Japan
GS1 South Korea
GS1 Taiwan (EAN)
GS1 US
IBM
Impinj
Infineon Technologies NA Corp
Institute for Information Industry
Intelleflex
Intermec
Internet Initiative Japan, Inc.
Johnson & Johnson
Kimberly-Clark Corp
KL-NET
Korea Computer Servs, Ltd
LIT (Research Ctr for Logistics Info Tech)
Loftware, Inc.
Manhattan Associates
MET Labs
Metarights
Metro

Microelectronics Technology, Inc.
Mstar Semiconductor
NCR
NEC Corporation
NXP Semiconductors
OatSystems
ODIN Technologies
Omron
Oracle Corporation
Panda Int'l Transp Ltd
Pango Networks, Inc.
Paxar
PepsiCo
Polaris Networks
Procter & Gamble
Psion Teklogix Inc.
Q.E.D. Systems
Raining Data Corporation
RetailTech
Reva Systems
RFIP Ltd. (formerly Radio Freq Ident Ctr)
RFXCEL Corp
Savi Technology
Sirit
SOFTBANK TELECOM Corp. (Japan)
Supply Insight, Inc.
SyGade Solutions
Symbol Technologies, Inc.
T3C Incorporated
Tagent Corporation
TagSys
TEGO, Inc.
ThingMagic, LLC
Tibco
Toppan Printing Co

Toray International, Inc.
Tyco / ADT
Ussen Limited Company
VeriSign
Vocollect
Vue Technology
Wal-Mart
Wish Unity
Yuen Foong Yu Paper