

December 6, 2006

Press Release

T-Engine Forum  
Ubiquitous ID Center

## **Authorized $\mu$ -Chip Hibiki as a ucode tag by Ubiquitous ID Center**

### **•01-010 $\mu$ -Chip Hibiki (Hitachi, Ltd.)**

The T-Engine Forum, an organization for the standardization and promotion of basic ubiquitous computing technology (Location: Shinagawa Ward, Tokyo, Chair: Ken Sakamura, Professor at the University of Tokyo/Chair of the Ubiquitous ID Center, Number of members: 492) has been advancing the deployment of open infrastructure systems that realize free mobility assistance functions. In these systems, unique numbers called "ucodes" are attached to physical objects and locations using RFIDs and active tags which have infrared or radio communication functions, etc. These ucodes are read with a portable device called the "Ubiquitous Communicator". Using information related to physical objects and locations and information acquired from ucodes, new applications are now possible. For example, T-Engine forum has been developing technology to be used as the open technology infrastructure for free mobility assistance functions that can support supply chain management, traceability, and navigating and sightseeing guidance. The Ubiquitous ID Center within the T-Engine Forum authorizes specifications for RFID tags and radio wave markers, and issues unique numbers for these infrastructure systems so that they are widely used and available.

The Ubiquitous ID Center ([www.uidcenter.org](http://www.uidcenter.org)) authorized a passive RFID tag (860-960MHz) compatible with ucode, " $\mu$ -Chip Hibiki" from Hitachi Ltd. as a ucode-compatible RFID tag. The Ubiquitous ID Center will use it for each demonstration experiment. Also, they will examine if it can be applied to a part of ubiquitous ID architecture solution.

#### **Authorization Number: 01-010 " $\mu$ -Chip Hibiki" (Hitachi Ltd.)**

" $\mu$ -Chip Hibiki" of Hitachi Ltd. is a passive RFID (860 to 960MHz, ISO18000-6 Type C). It has been authorized as Interface Category 1\*1 and Security Class 0\*2.

The Ubiquitous ID Center authorizes various types of tags and classifies them into interface categories and security classes according to their intended use so that users can use the most appropriate tag for their applications.

For the authorization of "μ-Chip Hibiki" this time, the interim method of identifying ucode and other codes was used. The standard method as an international standard is being currently discussed with the relative authorities in consideration of obtaining AFI (Application Family Identifier) which is the standard method of identifying electronic tag codes compatible with ISO 18000-6 Type C such as "μ-Chip Hibiki".

**[Inquiries regarding this issue]**

T-Engine Forum Ubiquitous ID Center (Contact: Mr. Koshizuka)  
 Tel: 03-5437-2290 e-mail: [press@t-engine.org](mailto:press@t-engine.org)

**[Terms description and remarks]**

**\*1 Physical Layer Category**

The Ubiquitous ID Center defined the interface categories based on the physical layer interface for ucode tag communication as shown in Table 1:

Table1 Interface Categories for ucode Tags

Category	Contents
Category 0	Print tag (bar code, two-dimensional bar code)
Category 1	RF tags (RFID tags with a contactless interface and a contactless IC card)
Category 2	Active RF tags (RFID tags and sensor nodes that have batteries and communicate using RF)
Category 3	Active infrared tags (ID tags and sensor nodes that have batteries and communicate using infrared light)

**\*2 Security Class**

The Ubiquitous ID Center defined the security classes based on the security to be satisfied by ucode tags as shown in Table 2:

Table 2 Security Classes for ucode Tags

Class	Provided security-related features
Class 0	Data defect detection (Damage caused in a part of data due to disturbance or physical defects in optical tags can be detected.)
Class 1	Physical duplication resistant/Physical forgery resistant (Creating data which is physically identical or similar is difficult)
Class 2	Identification prevention (Identification of communication status, contents and methods is prevented)
Class 3	Tamper-resistant, access management by resource (Information stored in tags cannot be read physically or logically. Also, controls access to each stored resource according to authority class of access of logical resource resistance.)

Class 4	Secure communications with unknown nodes (A secure data communication path can be established even for an unidentified node that has not previously shared a private key when exchanging tag data via a network.)
Class 5	Time-dependent resource management (Time-limit management for carrier's data, security information and tag feature operation can be conducted, such as setting up a data validity period or stopping an operation after a certain period of time.)
Class6	Internal program/security information update (Maintenance function that enables maintenance of the optimum security status for how it is used, such as updating firmware or applying a security patch).