

Jan 30, 2020

## Panasonic Develops Multifunctional Secure IC that Protects Critical Data on IoT and Industrial Devices

Panasonic has developed a multifunctional secure IC and will start sample shipments in February 2020. This product, which is simple to install, improves the security of IoT and industrial devices.

**Osaka, Japan** – Panasonic Corporation today announced it has developed a multifunctional secure IC in response to the need for enhanced security measures to protect IoT and industrial devices used in facilities such as factories and warehouses. When installed in such devices, via a simple process, this new secure IC with unique encrypting functions will boost their security. The company will start sample shipments in February 2020.

The use of IoT devices has been growing rapidly in a variety of fields, requiring improved measures against increasingly sophisticated and diverse security attacks. Conventionally, an authentication key is written from outside the IC and retained in the IC. Panasonic's new product, however, generates and retains a unique authentication key inside the IC and deletes it after use, blocking any interception of the key and effectively protecting important data. Equipped with NFC [1], a wireless interface function, and a memory (ReRAM [2]) that is highly resistant to radiation, the new multifunctional secure IC is also applicable to devices not connected to the internet and medical devices. The product further secures the safety of the device over its entire life cycle, from manufacture to disposal or reuse, in addition to during use, contributing to achieving safe and secure IoT systems.

Panasonic's new multifunctional secure IC has the following features.

1. Improving the security resistance of data by generating and deleting a unique authentication key inside the IC each time.
2. Equipped with NFC, a wireless interface function, and ReRAM that is highly resistant to radiation.
3. Improving the safety of devices over their entire life cycle through cooperation with trust service providers [3].

### Conventional example

Previously, the authentication key of a device was written from outside the IC to the memory inside the IC. This raised a risk of the authentication key being intercepted, so the customer side was responsible for creating a safe environment. There was also a risk of data in the memory being intercepted or tampered with.

### Suitable applications

- IoT and industrial devices in general (logistics, smart factories, network devices, etc.)
- Management of medical equipment and pharmaceuticals to be sterilized by radiation

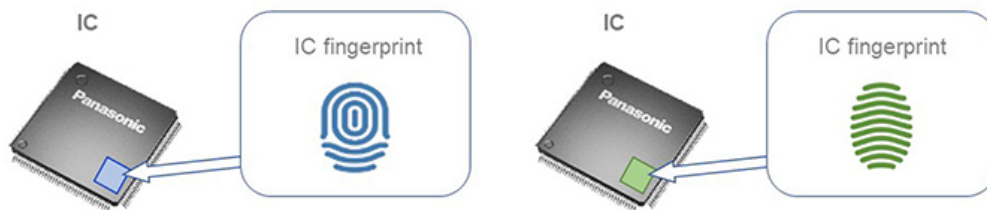
## Product features

### 1. Improving the security resistance of data by generating and deleting a unique authentication key inside the IC each time

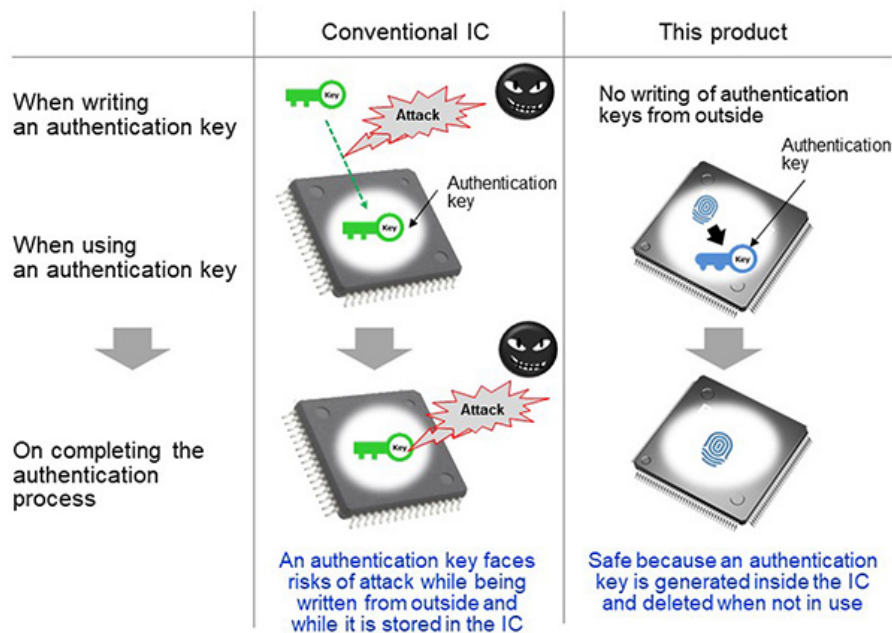
As a unique security function, Panasonic's multifunctional secure IC possesses IC-specific analog information, which is different for each IC. This analog information (IC fingerprint) is unique in the same way as human biological information (fingerprint). The IC fingerprint is analog and therefore cannot be copied.

Resistance to interception and tampering with data in the memory is thereby enhanced because this product generates a unique authentication key from an IC fingerprint and uses the authentication key to encrypt important data in the memory. This product significantly upgrades security and is resistant to tampering, because it also generates an authentication key from the IC fingerprint when authenticating the device, and deletes the authentication key on completion of the authentication process.

#### [Each IC's fingerprint is different]



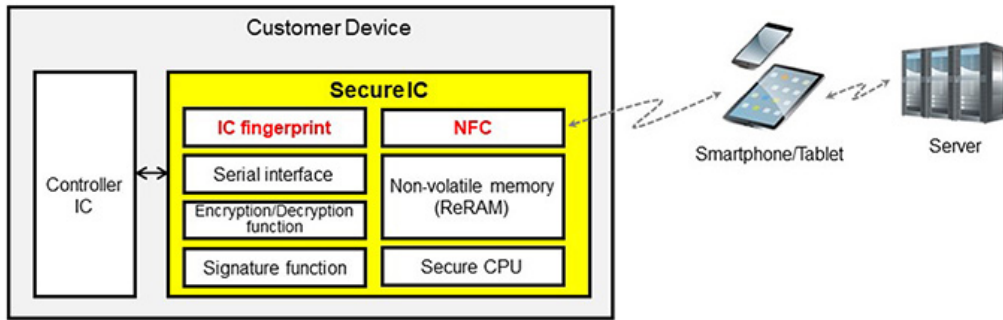
#### [Safe because an authentication key is generated from an IC fingerprint and then deleted after completing the authentication process]



### 2. Equipped with NFC, a wireless interface function, and ReRAM that is highly resistant to radiation

This product is equipped with NFC for wireless communications, enabling even devices that are not already connected to the internet to get internet connection via smartphones and tablets. This allows for the mutual authentication of devices using the server, preventing impersonation. The use of an energy harvesting function [4] allows smartphones and tablets to read controller IC information and security incident records in the devices and to configure device operation settings via NFC even when the device power is off. This will facilitate system maintenance management and improve usability.

**[Example of NFC use]**



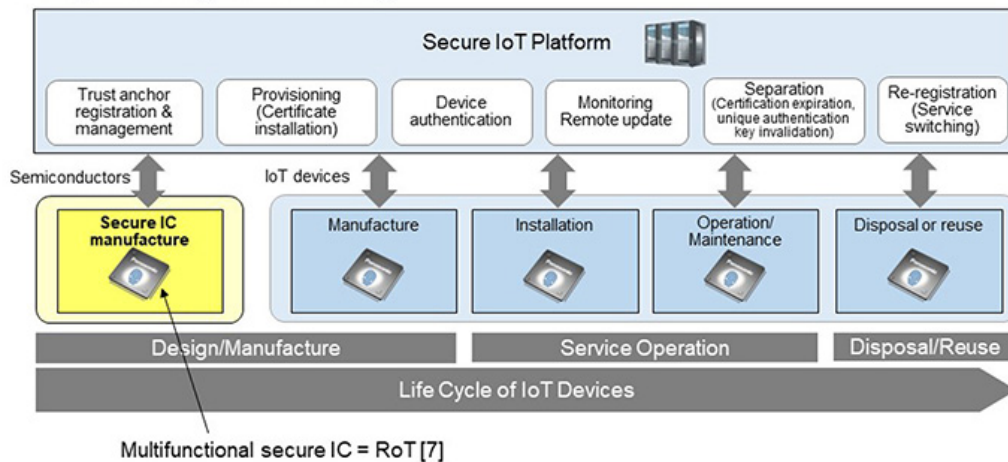
This product is equipped with ReRAM, a non-volatile memory that is highly resistant to radiation, making it also usable for management of medical equipment and pharmaceuticals to be sterilized by radiation.

**3. Improving the safety of devices over their entire life cycle through cooperation with trust service providers.**

This product is equipped with a function compatible with secure IoT platforms of trust service providers\*. Incorporating this product, which possesses a trust anchor [5], into IoT devices and executing certificate-based authentication, ensures the safety of devices over their entire life cycle, from manufacture to disposal or reuse, helping to achieve safe and secure IoT systems. This also facilitates compliance with the security standards that govern control systems, specified in IEC62443 [6].

\*As of January 30, 2020, Panasonic is examining the possibility of development cooperation with Cybertrust Japan Co., Ltd.

**[Example of Ensuring the Safety of IoT Devices over their Entire Life Cycle Using this Product]**



## Basic specifications

SecureIC (Part No.: MN67S3C0 Series)		
Manufacturing process		40-nm embedded ReRAM
CPU Core	ARM SC000	Max. 40 MHz
Interface	SPI	2ch (Single/Quad×1ch+Single×1ch) Max. 40 Mbps
	I2C	Fast mode (400 kbps)
	NFC	ISO/IEC 14443 Type A ISO/IEC 14443 Type B JISX6319-4 FeliCa (Note)
Memory	ReRAM memory	256 KB
	RAM	16 KB
Cryptography (Common key)	DES	Key length 112
	AES	Key length 128/192/256
Cryptography (Public key)	RSA	Key length 1024/2048/3072/4096
	ECC	Key length 160/224/256/521
HASH		SHA-1/SHA-2
CC Certification (Hardware)		EAL5+

Note) FeliCa is a contactless IC card technology system developed by Sony Corporation and is a registered trademark of Sony Corporation.

## Description of terms

### [1] NFC

Abbreviation of Near Field Communication, which refers to short-range wireless communication standards specified by the International Organization for Standardization (ISO).

### [2] ReRAM

Abbreviation of resistive random access memory. A type of non-volatile memory which records "0" and "1" digital bits by generating large resistance changes using a pulsed voltage applied to a thin-film metal oxide. The simple structure of a metal oxide sandwiched by electrodes makes the manufacturing process easier and provides excellent low power-consumption and high-speed rewriting characteristics.

### [3] Trust service provider

A trust service provider in IoT services provides a framework which is the foundation for ensuring the effectiveness of systems by ensuring authenticity through the authentication of IoT devices and verification of user identification, ensuring integrity through the detection of data tampering, etc.

### [4] Energy harvesting function

A technology for obtaining electric power by harvesting energy such as sunlight, artificial light, and machine-generated vibrations and heat. Here, it refers to a function that obtains electric power from electromagnetic waves generated by tablets and smartphones equipped with an NFC function.

### [5] Trust anchor

In this context, this term refers to information (unique authentication keys and ID information) used for electronic certificates. Storing this information at the RoT forms the basis of trust for electronic authentication.

### [6] IEC62443

The standards of security management systems related to control systems, specified by the International Electrotechnical Commission (IEC).

### [7] RoT

Abbreviation of Root of Trust, which here refers to secure ICs that store important information such as unique authentication keys and electronic certificates.

## For product inquiries, contact:

Panasonic Semiconductor Solutions Co., Ltd.

<https://www.panasonic.com/jp/company/pscs/en/contact.html?ad=press20200130>

## About Panasonic

Panasonic Corporation is a worldwide leader in the development of diverse electronics technologies and solutions for customers in the consumer electronics, housing, automotive, and B2B businesses. The company, which celebrated its 100th anniversary in 2018, has expanded globally and now operates 582 subsidiaries and 87 associated companies worldwide, recording consolidated net sales of 8.003 trillion yen for the year ended March 31, 2019. Committed to pursuing new value through innovation across divisional lines, the company uses its technologies to create a better life and a better world for its customers. To learn more about Panasonic: <https://www.panasonic.com/global>.

*\*The content in the following news releases is accurate at the time of publication but may be subject to change without notice. Please note therefore that these documents may not always contain the most up-to-date information.*