

## **Application Note**

# **V850**

## **32-Bit Single-Chip Microcontrollers**

## **AES 128 Encryption/Decryption**

---

## **DISCLAIMER**

The related documents in this application note may include preliminary versions. However, preliminary versions may not have been marked as such.

The information in this application note is current as of its date of publication. The information is subject to change without notice. For actual design-in, refer to the latest publications of NEC's data sheets or data books, etc., for the most up-to-date specifications of PRODUCT(S). Not all PRODUCT(S) and/or types are available in every country. Please check with an NEC sales representative for availability and additional information.

No part of this application note may be copied or reproduced in any form or by any means without prior written consent of NEC. NEC assumes no responsibility for any errors that may appear in this application note. NEC does not assume any liability for infringement of patents, copyrights or other intellectual property rights of third parties by or arising from the use of PRODUCT(S) listed in this application note or any other liability arising from the use of such PRODUCT(S).

No license, express, implied or otherwise, is granted under any patents, copyrights or other intellectual property rights of NEC or others. Descriptions of circuits, software and other related information in this application note are provided for illustrative purposes of PRODUCT(S) operation and/or application examples only. The incorporation of these circuits, software and information in the design of customer's equipment shall be done under the full responsibility of customer. NEC assumes no responsibility for any losses incurred by customers or third parties arising from the use of these circuits, software and information.

While wherever feasible, NEC endeavors to enhance the quality, reliability and safe operation of PRODUCT(S) the customer agrees and acknowledges that the possibility of defects and/or erroneous thereof cannot be eliminated entirely. To minimize risks of damage to property or injury (including death) to persons arising from defects and/or errors in PRODUCT(S) the customer must incorporate sufficient safety measures in their design, such as redundancy, fire-containment and anti-failure features.

The customer agrees to indemnify NEC against and hold NEC harmless from any and all consequences of any and all claims, suits, actions or demands asserted against NEC made by a third party for damages caused by one or more of the items listed in the enclosed table of content of this application note for PRODUCT(S) supplied after the date of publication.

PRODUCT(S) are classified into the following three quality grades: "Standard", "Special" and "Specific". The "Specific" quality grade applies only to PRODUCT(S) developed based on a customer-designated "quality assurance program" for a specific application. The recommended applications of PRODUCT(S) depend on its quality grade, as indicated below. Customers must check the quality grade of each PRODUCT(S) before using it in a particular application.

- "Standard": Computers, office equipment, communications equipment, test and measurement equipment, audio and visual equipment, home electronic appliances, machine tools, personal electronic equipment and industrial robots
- "Special": Transportation equipment (automobiles, trains, ships, etc.), traffic control systems, anti-disaster systems, anti-crime systems, safety equipment and medical equipment (not specifically designed for life support).
- "Specific": Aircraft, aerospace equipment, submersible repeaters, nuclear reactor control systems, life support systems and medical equipment for life support etc.

The quality grade of PRODUCT(S) is "Standard" unless otherwise expressly specified in NEC data sheets or data books, etc. If customers wish to use PRODUCT(S) in applications not intended by NEC, they must contact NEC sales representative in advance to determine NEC's willingness to support a given application.

If the supplied goods/information are subject to Japanese, German, European and/or North American export controls, the customer shall comply with the relevant export control regulations in the event that the goods are exported and/or re-exported. If deliveries are exported without payment of duty at the request of the customer, the customer accepts liability for any subsequent customs administration claims with respect to NEC.

**Notes:** (1) "**NEC**" as used in this statement means NEC Electronics Corporation and also includes its direct or indirect owned or controlled subsidiaries.

(2) "**PRODUCT(S)**" means any product developed or manufactured by or for NEC (as defined above).

## Table of Contents

Chapter 1 Supporting Data Security .....	4
Chapter 2 Revision History .....	5

## Chapter 1 Supporting Data Security

NEC Electronics Europe (GmbH) has ported the Rijndael ANSI C code by Rijmen, Bosselaers and Barreto to our 32-bit V850 microcontroller, with a view to providing unrestricted AES128 middleware libraries free-of-charge to designers using, what is today, the world's number one selling 32-bit microcontroller. (Source: Gartner Dataquest, April 2008).

There are three main components included in the library:

- Source code of the encryption, decryption routines.
- Associated header file for the above.
- Test routines to verify the execution speed of the routines provided.

The software supports encryption key lengths of 128-bits, 192-bits and 256-bits and can be used with any V850 family microcontroller.

Implementing the library is very straightforward, following this simple process:

- Call a function that initialises the key that will be used to encrypt and decrypt the messages; you just need to pass the size of the key (128-, 192- or 256-bits) to the library function provided.
- Call a function to encrypt a 128-bit message; the result is a 128-bit encrypted message.
- Call the decrypt function.

Two test functions are also provided by NEC Electronics. The first, called SimpleAESTest, performs three encryptions / decryptions with three different key sizes (128-, 192- and 256-bits). Comparison is performed to verify that the result of each of these three encryptions / decryptions gives back the plaintext as well as measuring the encryption / decryption timings for each key size. The second function, ValidAES, performs a deeper validation of the Rijndael implementation using externally validated test vectors. Details on this validation method can be found on the Internet at

[http://blogs.msdn.com/si\\_team/archive/2006/05/19/602055.aspx](http://blogs.msdn.com/si_team/archive/2006/05/19/602055.aspx).

**It goes without saying that responsibility for the actual implementation lies with the user of the middleware.**

In terms of resource required, our middleware requires 4,494 bytes of code memory, 4,096 bytes of data memory and 10,376 bytes of constant memory, based on its usage in a V850 32-bit microcontroller.

It should be noted that whilst developed with a 32-bit microcontroller in mind, given the availability of 'C' source code in NEC Electronics' library, it would be practical to easily port the code to a 16-bit or even an 8-bit microcontroller, although the required response time should be considered as the CPU clock speed of the selected NEC Electronics microcontroller decreases.

Further details are available by contacting NEC Electronics at [www.eu.necel.com](http://www.eu.necel.com).

## Chapter 2 Revision History

Item	Date published	Document No.	Comment
1	January 22, 2009	U19668EE1V0AN00	1 <sup>st</sup> Release