

---

# Randomization Services Reference

Security



2008-03-12



Apple Inc.  
© 2008 Apple Inc.  
All rights reserved.

you specific legal rights, and you may also have other rights which vary from state to state.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, mechanical, electronic, photocopying, recording, or otherwise, without prior written permission of Apple Inc., with the following exceptions: Any person is hereby authorized to store documentation on a single computer for personal use only and to print copies of documentation for personal use provided that the documentation contains Apple's copyright notice.

The Apple logo is a trademark of Apple Inc.

No licenses, express or implied, are granted with respect to any of the technology described in this document. Apple retains all intellectual property rights associated with the technology described in this document. This document is intended to assist application developers to develop applications only for Apple-labeled computers.

Apple Inc.  
1 Infinite Loop  
Cupertino, CA 95014  
408-996-1010

Apple and the Apple logo are trademarks of Apple Inc., registered in the United States and other countries.

IOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license.

Even though Apple has reviewed this document, APPLE MAKES NO WARRANTY OR REPRESENTATION, EITHER EXPRESS OR IMPLIED, WITH RESPECT TO THIS DOCUMENT, ITS QUALITY, ACCURACY, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. AS A RESULT, THIS DOCUMENT IS PROVIDED "AS IS," AND YOU, THE READER, ARE ASSUMING THE ENTIRE RISK AS TO ITS QUALITY AND ACCURACY.

IN NO EVENT WILL APPLE BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM ANY DEFECT OR INACCURACY IN THIS DOCUMENT, even if advised of the possibility of such damages.

THE WARRANTY AND REMEDIES SET FORTH ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHERS, ORAL OR WRITTEN, EXPRESS OR IMPLIED. No Apple dealer, agent, or employee is authorized to make any modification, extension, or addition to this warranty.

Some states do not allow the exclusion or limitation of implied warranties or liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you. This warranty gives

# Contents

## **Randomization Services Reference 5**

---

- Overview 5
- Functions 5
  - SecRandomCopyBytes 5
- Data Types 6
  - SecRandomRef 6
- Constants 6
  - Number Generator Default 6

## **Document Revision History 7**

---



# Randomization Services Reference

---

<b>Framework:</b>	Security/Security.h
<b>Declared in</b>	SecRandom.h

## Overview

Randomization Services is an API that generates cryptographically secure random numbers.

## Functions

### SecRandomCopyBytes

Generates an array of cryptographically secure random bytes.

```
int SecRandomCopyBytes (  
    SecRandomRef rnd,  
    size_t count,  
    uint8_t *bytes  
);
```

#### Parameters

*rnd*

The random number generator object to use. Specify `kSecRandomDefault` to use the default random number generator.

*count*

The number of random bytes to return in the array pointed to by the *bytes* parameter.

*bytes*

The random bytes generated by the function.

#### Return Value

Returns 0 if the function completed successfully and -1 if there was an error. Check the `errno` system variable for the error.

#### Discussion

This function reads from `/dev/random` to obtain an array of cryptographically-secure random bytes. For more information on the `/dev/random` random-number generator, see the manual page for `random(4)`.

#### Availability

Available in iOS 2.0 and later.

**Related Sample Code**  
CryptoExercise

**Declared In**  
SecRandom.h

## Data Types

### SecRandomRef

Abstract Core Foundation-type object containing information about a random number generator.

```
typedef const struct __SecRandom * SecRandomRef;
```

**Availability**  
Available in iOS 2.0 and later.

**Declared In**  
SecRandom.h

## Constants

### Number Generator Default

Indicates the default random number generator.

```
const SecRandomRef kSecRandomDefault;
```

#### Constants

`kSecRandomDefault`

When passed to the [SecRandomCopyBytes](#) (page 5) function as the random number generator reference, this constant indicates that the default number generator should be used.

This constant is a synonym for `NULL`.

Available in iOS 2.0 and later.

Declared in `SecRandom.h`.

# Document Revision History

---

This table describes the changes to *Randomization Services Reference*.

Date	Notes
2008-03-12	New document that describes an API to generate random numbers.

## REVISION HISTORY

### Document Revision History