NAME

    RSA_blinding_on, RSA_blinding_off - protect the RSA operation from timing attacks

SYNOPSIS

    #include <openssl/rsa.h>

    The following functions have been deprecated since OpenSSL 3.0, and can be hidden entirely by defining **OPENSSL_API_COMPAT** with a suitable version value, see **openssl_user_macros**(7):

    int RSA_blinding_on(RSA *rsa, BN_CTX *ctx);

    void RSA_blinding_off(RSA *rsa);

DESCRIPTION

    All of the functions described on this page are deprecated.

    RSA is vulnerable to timing attacks. In a setup where attackers can measure the time of RSA decryption or signature operations, blinding must be used to protect the RSA operation from that attack.

    RSA_blinding_on() turns blinding on for key **rsa** and generates a random blinding factor. **ctx** is **NULL** or a preallocated and initialized **BN_CTX**.

    RSA_blinding_off() turns blinding off and frees the memory used for the blinding factor.

RETURN VALUES

    RSA_blinding_on() returns 1 on success, and 0 if an error occurred.

    RSA_blinding_off() returns no value.

HISTORY

    All of these functions were deprecated in OpenSSL 3.0.

COPYRIGHT

    Copyright 2000-2021 The OpenSSL Project Authors. All Rights Reserved.

    Licensed under the Apache License 2.0 (the "License"). You may not use this file except in compliance with the License. You can obtain a copy in the file LICENSE in the source distribution or at <https://www.openssl.org/source/license.html>.