|  |  |
| --- | --- |
| W3C | **The World Wide Web Consortium (W3C)** |
| TPAC 2013October 29- November 2 2012, Lyon, France | **Original: English** |
| **WG:** | Security Activity | Web CryptoAPI Working Group |
|  | PROPOSAL CONTRIBUTION |
| **Authors:** | Jonghong Jeon, ETRI, (hollobit@etri.re.kr) Mountiee Lee, Paygate (mountie@paygate.net) |
| **Title:** | **Propose to adding text in Section 23 Algorithms** |

Copyright © 2012 ETRI. All rights reserved. This document is available under the W3C Document License. See the W3C Intellectual Rights Notice and Legal Disclaimers for additional information.

1. Overview

This proposal proposes to add text for the SEED algorithm in Section 23 Algorithms and Section 27 References

1. Proposed adding text in Section 23

23.16. SEED

**23.16.1. Description**

This “SEED” a 128-bit symmetric key block cipher that has been developed by KISA (Korea Information Security Agency) since 1998, as specified by [RFC4269]. SEED is a national standard encryption algorithm in the Republic of Korea [TTASSEED] and is designed to use the S-boxes and permutations that balance with the current computing technology,

**23.16.2. Registration**

The [recognized algorithm name](http://www.w3.org/TR/WebCryptoAPI/#recognized-algorithm-name) for this algorithm is "SEED".

| [**Operation**](http://www.w3.org/TR/WebCryptoAPI/#supported-operations) | [**Parameters**](http://www.w3.org/TR/WebCryptoAPI/#algorithm-specific-params) | [**Result**](http://www.w3.org/TR/WebCryptoAPI/#algorithm-result) |
| --- | --- | --- |
| encrypt | [SeedCbcParams](http://www.w3.org/TR/WebCryptoAPI/#dfn-RsaOaepParams) | ArrayBufferView? |
| decrypt | [SeedCbcParams](http://www.w3.org/TR/WebCryptoAPI/#dfn-RsaOaepParams) | ArrayBufferView? |
| generateKey | [SeedKeyGenParams](http://www.w3.org/TR/WebCryptoAPI/#dfn-RsaKeyGenParams) | Key? |

#### 23.16.3. SeedCbcParams dictionary

**IDL**

dictionary *SeedKeyGenParams* : [AlgorithmParameters](http://www.w3.org/TR/WebCryptoAPI/#dfn-AlgorithmParameters) {

 // Seed Key length, in bits, of the key

 [EnforceRange] unsigned short length;

};

dictionary SeedCbcParams : AlgorithmParameters {

 // The initialization vector. MUST be 16 bytes.

 ArrayBufferView iv;

}

#### 23.16.4. Operations

* Encrypt
* Decrypt
* Generate Key
1. Proposed adding text in Section 27 References

**RFC4269**

[*The SEED Encryption Algorithm*](http://www.ietf.org/rfc/rfc3447), H.J. Lee, S.J. Lee, J.H. Yoon, D.H. Cheon, J.I. Lee, KISA, IETF.