Contents

1 Preface

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

2 Hash algorithm

Identifier	Algorithm name	Remarks
0000 - fdff	*Unallocated*	
fe00 - feff	Implementation specific algorithm	[1]
ff00 - ffff	Reserved for future expansion	

1. Implementations MAY use this block of identifiers for algorithm that does not have any identifier allocated to it.

3 Encryption algorithm

Identifier	Cipher Type	Algorithm name	Remarks
0000 - 4fff		*Unallocated*	
5000	BLOCK	Null cipher	[1]
5001	STREAM	Null cipher	[1]
5002 - fdff		*Unallocated*	
fe00 - frff		Implementation specific algorithm	[2]
ff00 - ffff		Reserved for future expansion	

1. Null cipher is not recommended to be used as it does not actually encrypt the data. Implementation SHOULD provide warning for using these cipher.

2. Implementations MAY use this block of identifiers for algorithm that does not have any identifier allocated to it.

4 Key derivation algorithm

Identifier	Algorithm name	Remarks
0000 - fdff	*Unallocated*	
fe00 - feff	Implementation specific algorithm	[1]
ff00 - ffff	Reserved for future expansion	

1. Implementations MAY use this block of identifiers for algorithm that does not have any identifier allocated to it.