Comments from the IEEE P1619.1 Task Group Concerning NIST SP 800-38D July 2007 Draft

To: Morris Dworkin, NIST
From: Matthew V. Ball, IEEE P1619.1 Task Group Chair
Date: July 30, 2007

Overview

This memo contains comments from the IEEE P1619.1 Task Group concerning the July 2007 draft of NIST Special Publication 800-38D "*Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication*". The IEEE P1619.1/D22 draft standard includes four cryptographic modes of operation, one of which is GCM. Up through draft P1619.1/D21, the P1619.1 Task Group was using the April 2006 SP 800-38D draft as a normative reference for GCM in anticipation of the draft correcting technical discrepancies with the original submission document. The P1619.1/D22 draft now uses the original McGrew/Viega GCM submission as the normative reference for GCM. We hope that the final SP 800-38D standard can stay consistent with both the original GCM submission, and the IEEE P1619.1 draft standard, if possible. Many GCM implementations are based on these documents, and these implementations might be unable to easily change to match the current 800-38D draft.

The following comments are based on discrepancies between P1619.1/D22 and the latest SP 800-38D draft.

Technical Comments

1. Section 9.1 requires that the GCM implementation be FIPS 140-2 compliant. Please consider removing all references to FIPS 140-2 from SP 800-38D for the following reasons:
    1. Other standards (e.g. IEEE P1619.1 or RFC 4106) may reference 800-38D for GCM but may not have requirements that the implementation be FIPS 140-2 compliant.
    2. These references will soon be out-of-date when FIPS 140-3 is released.
    3. It is unprecedented for the previous 800-38 standards to mention FIPS 140-2.
    4. The relationship between FIPS 140-2 and the SP 800-38 series documents should be unidirectional: that is, FIPS 140-2 could reference an 800-38 mode as 'Approved', but the modes themselves should not reference FIPS 140-2. Otherwise, you open the door to strange compliance issues that may make it impossible to be compliant to either standard (can a FIPS 140-3 implementation use GCM? It's not FIPS 140-2-compliant...)
2. If SP 800-38D needs to reference FIPS 140-2, then please consider making FIPS 140-2-compliance optional, and instead state something like this: "If the GCM

implementation is FIPS 140-2-compliant, then the following requirements apply: (list FIPS requirements such as documentation, critical security parameters, cryptographic boundary, etc)"

3. In 8.1 "Deterministic Construction", it would be useful to reiterate that the requirements of unique IVs only apply when using the same cryptographic key in two or more devices. If the cryptographic module generates its own key, then the 'fixed field' could be zero-bits in length, and the 'counter field' could consume the entire IV (because the cryptographic module could ensure that no two devices use the same key).
4. In 8.2 "RBG-Based Construction", consider allowing implementations that start with a random number, and then increment this random number with each successive encrypted record. Such implementations can still meet the requirement of Section 9 that the chance of an IV-collision is no greater than 1 in 2^{32}.
5. This latest draft removed the allowance for IVs other than 96-bits. The P1619.1/D22 draft allows 128-bit or larger IVs and we have confirmed that there are implementations that use such large IVs. Since it is possible to meet the (Section 9) uniqueness requirements with large IVs, we recommend adding support for large IVs back into the standard, using the original algorithm in the McGrew and Viega submission (not the algorithm of the previous SP 800-38D draft). We do not know of any implementations that use IVs smaller than 128-bits, except for the default of 96-bits, so it should be fine to require that large IVs contain at least 128 bits.

Editorial Comments

1. In Section 9, the word 'must' should be replaced with 'shall' ('shall' is defined as a keyword that carries conformance requirements – 'must' carries no such requirements).