Hello NIST,

We are currently implementing GCM in accordance with RFC 4106 which covers The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP). A requirement exists to be compliant with SP800-38D when it's published.

On the June draft I have the following three queries:

1. We are using Deterministic Construction as specified in Section 9. Our fixed field is made up of 4 bytes of GCM Salt that is created during the Key Exchange Process (in accordance with RFC 4106). The Key Exchange process uses Certificates to verify the parties involved for each Secure Association. A different GCM Salt value is used for each Secure Association. On this basis do we meet the requirement stated at the beginning of section 8.1:

In the deterministic construction, the IV is the concatenation of two fields, called the fixed field and the counter field. The fixed field shall identify the device, or, more generally, the context, in which the authenticated encryption function is implemented.

My understanding is that this meets the ' or more generally, the context in which the authenticated encryption function is implemented'. Can you confirm?

2. Our symmetric key is held in volatile RAM so when there is a power outage the key is lost and a new one must be created to facilitate further encrypted messages on power up. A new fixed field and counter field are created at this point. Is this a permissible solution to the statement in the third paragraph of Section 9.1?:

The IV construction that is implemented from Sec. 8 above affects the options for recovery from a loss of power. For the deterministic construction, all of the deterministic elements that are necessary to construct the IV would have to be available when power is restored. For example, these elements could be stored in non-volatile memory.

This appears to be at odds with Design Consideration 2 in 9.1 which states:

A loss of power to the module shall not cause the repetition of IVs. If the generation unit cannot recover from a loss of power, then the device shall enter a failure state until a new key can be established. In this case, the new key shall be fresh, i.e., different than any previous key.

If the new key scenario is acceptable perhaps the statements could be made clearer.

3. Is SP800-38D draft June 2007 still completely consistent with RFC 4106?

My only other comment from reviewing the doc is:

* Consideration should be given to reversing Sections 8 and 9 as 9 is the requirement and 8 specifies how it's achieved. It then flows logically.

Regards,

Ian Clover

Ian Clover, Security Engineer
Thales e-Security Ltd