Comments Received on SP 800-131A, Revision 2
Transitioning the Use of Cryptographic Algorithms and Key Lengths
(comment period closed September 7, 2018)

Contents

Tom Arnold, IBM

From: Todd Arnold <arnoldt@us.ibm.com>
Date: Thursday, July 19, 2018 at 10:49 AM

I took a quick look at the revised document, and I think it is good. The retirement/deprecation of some algorithms, modes, and key lengths will make a lot of people unhappy, of course, but I think they are reasonable.

There is always a problem because the NIST requirements are consistently stronger than those of the financial industry. For example, 2-key TDES is still the predominant symmetric algorithm used in payments systems, and it will be quite a while before those migrate to AES. Also, EMV issues an annual "RSA key length assessment" (copied below) and their latest one says that it's OK to use 1408-bit RSA keys through 2024, and to use 1984-bit keys through 2028. I understand that SP 800-131 is for government applications and not payments, but the conflict causes confusion for people who have no choice but to use weaker algorithms, and who see that NIST says those are disallowed. Can you think of anything you could put in SP 800-131 that might help people understand all of this? I can't think of a good (or appropriate) way to do that, but I thought I'd ask.
Done..

I do have one specific suggestion. In light of the work toward quantum-resistant algorithms, I think it would be good to say something about the use of dual-signature methods, where one signature is computed using an approved algorithm (e.g. ECC) and the other is computed on the same data using an as-yet-unapproved QR algorithm. You could explain the rationale for doing this and say that it is acceptable because the approved algorithm makes it acceptable - and that the QR algorithm used in parallel does not make it become unacceptable.
This doesn't belong in 800-131A but might be a comment that could be considered when FIPS 186-5 is available for comment.

You always write the clearest and most understandable crypto standards - thank you for that.

James Larson, HUD

From: "Larson, James K" <James.K.Larson@hud.gov>
Date: Thursday, July 19, 2018 at 12:18 PM
To: cryptotransitions <cryptotransitions@nist.gov>
Cc: "Larson, James K" <James.K.Larson@hud.gov>
Subject: SP 800-131A comments

Thank you for the opportunity to provide feedback on the Draft Special Publication (SP) 800-131A Revision 2, Transitioning the Use of Cryptographic Algorithms and Key Lengths.
While reviewing the SP, I noticed that the spelling-out of abbreviations was not consistent. Some examples are: MAC, NIST, and SP are spelled out on first use; DH and MQV are spelled out on line 255, after having been used; and RSA is not spelled out. There are some others, as well. Although I realize that the normal reader of the SP will have a great depth of experience in the field, may I suggest the use of a glossary of the abbreviations which could assist some readers.
Done.

I hope that my feedback will help the team. I truly appreciate all of your hard work.

Thank you.

Jim

Joseph Latouf, CORAcsi

From: Joseph Latouf <jlatouf@coracsi.com>
Date: Monday, July 23, 2018 at 10:15 AM
To: cryptotransitions <cryptotransitions@nist.gov>

In your announcement and abstract, you identify the need to establish stronger keys and algorithms to adequately protect sensitive information as more powerful computing techniques evolve, including quantum computers.

Preamble:
Claude Shannon, the father of information theory, long ago established the concept of perfect encryption. This was in response to the One Time Pads (OTPs) that the Russians were using during WWII and subsequently the cold war (see Venona Project).
While an OTP represents perfect encryption, it cannot be reused and is not practical given 'pen and paper'.

Multiple Use Pads (MUPs):

- CORAcsi has pioneered the natural progression to OTPs in a digital world, namely, MUPs. We have removed the constraints that prevent our MUPs from being used time and again. MUPs are reusable, fast and practical in a digital environment.
- MUPs adhere to the concept of perfect encryption in the sense that there is no limit to the size of a MUP. Our MUPs start at 150 kB (1.2 million bits) which places them far beyond the capabilities of any algorithm or computer (including quantum computers).
- MUPs are not "block based" encryption, such as AES and every other standard on the market. MUPs give an attacker zero information, such as its size, or the boundary conditions (such as 256 bit keys – this block size is known to every attacker and cryptographer).
- MUPs are probabilistic in nature, rather than factorization based. This means that algorithms naturally suited to quantum computers (Shor and Grover's algorithms) are of no consequence to MUPs.

CORA blocs:

- bloc is an acronym for Binary Level Obfuscated Container. This is to clearly differentiate a CORA bloc from a "block" referred to above.

- CORA blocs are a distributed implementation similar to block chains, except that they are 'not' a decentralized, peer-to-peer implementation. Fine-grain Control is centrally maintained with the appropriate stake holder(s).

CORA:

- This technology combines MUPs and CORA blocs to empower unbreakable encryption today and tomorrow.
- Please note the inclusion of the word "empower" above. If CORA is properly implemented, then no one will break it. Unlike the Titanic which was advertised as unsinkable without a caveat about the Captain of the ship avoid collisions – CORA is unbreakable 'when properly implemented'.
- What would it take to break CORA? The attacker would have to obtain in their entirety, each and every one of the following:

1. The MUP.
2. The initialization data for this particular user/office.
3. Each CORA bloc – without exception – without corruption.
4. The CORA catalog for this solution.

Conclusion:
A new standard that is not based upon "factorization", nor "known block sizes or key sizes" is needed to ensure data security. Given that there are many highly intelligent mathematicians and technology experts, who are often highly motivated, a new standard of encryption cannot rely on mathematical complexity, but rather, probabilistic uncertainty. While CORA definitely satisfies these requirements, with or without CORA, these are the standards that will be needed as computational power continues to grow – especially as quantum computers enter the scene.
Thank you for your comment. NIST will consider for future work.

Best Regards,
Joseph Latouf

Christophe Goyet, IDEMIA

From: GOYET Christophe <christophe.goyet@idemia.com>
Date: Thursday, September 6, 2018 at 5:04 PM

Thank you for putting together an updated version of NIST SP 800-131A Rev 2.

IDEMIA (formerly Oberthur Technologies) has reviewed this draft in details and believes it goes in the right direction.
From a commercial standpoint, we fully support this move to depreciate or disallow the use of TDES.

Since 2014, all our smart cards (CMVP certifications # 2303, 2392, 2545, 2743, 2986 and 3039) have an AES 256 security architecture that includes a DRBG compliant with SP 800-

90A and are supporting RSA up to 2048 and ECC up to P-384, to allow our customers to remain compliant with SP800-131A rev 2.

IDEMIA smart card platforms go even further and already support RSA up to 4096 and ECC up to P-521 although these algorithms have not been made available to the end user for lack of a standardized algorithm identifier in the PIV specifications SP 800-78-4 table 6.2. To prepare migration to stronger algorithm, IDEMIA would welcome a revised version of SP800-78 that adds support for RSA 3072 and RSA 4096 as well as ECC P-521 in the NPIVP specifications.

Going back to this draft of SP800-131A rev 2, we were wondering why NIST has not published a depreciation date for AES 128 knowing that the NSA has removed AES-128 from its Suite B algorithm already two years ago, to provide cost effective security against a potential quantum computer.
NSA's requirements are more restrictive than most of the other government agencies. SP 800-131A does not prohibit stronger approved mechanisms.

Would NIST follows and start to depreciate AES-128 for some use cases to help the industry to be more proactive in its transition to stronger cryptographic algorithms and key lengths?
At this time, NIST is not planning to deprecate AES-128, since it appears adequate. However, NIST continues to observe attacks on its approved algorithms and will respond appropriately if and when a practical attack is found.

Please feel free to contact me should you wish to discuss the above.

Best Regards.

Christophe

Rene Struik

From: Rene Struik <rstruik.ext@gmail.com>
Date: 9/7/18, 1:36 PM

I just noticed that the comment period for NIST SP 800-131A - Rev2 is not 90 days (which I had assumed), but roughly half that time and officially is due today.

I intended to comment on this. If you will not be able to accept comments that come in, say, by end of this weekend or Monday coming up, please let me know. If you would be somewhat lenient, please let me know and I will produce these in the next 2 days or so.

FYI - One thing I just noticed is that in Rev1 DSA has minimum sizes for the ordinary DLP group Zp and the prime-order multiplicative subgroup of size q, whereas Rev2 nails this down to rigid numbers. I would like to

reflect on this somewhat more and see if this warrants a technical comment. Similarly, FIPS 186-4 allows curves besides the well-known NIST curves (which are labelled as recommended), while it is not clear whether other curves (such as the CFRG curves) for key agreement are allowed within the parameters of the 131a-rev2 draft doc.
These issues are in the purview of FIPS 186-5, which has not been posted for comment yet. It is premature to address in this revision of SP 800-131A.

Best regards, Rene