Public Comments on the Proposal to Approve EAX´

On June 21, 2011, NIST announced a period of public comment, ending July 22, 2011, on a proposal to approve the EAX´ mode of operation. The announcement was posted on the News and Events page at NIST's Computer Security Resource Center.

Below are the public comments that NIST received in response to this request.

Avygdor Moise

Approval of this mode will greatly enhance both the security and interoperability of ANSI C12.22/IEEE 1703 Nodes.

This also will help future proof the standard, given the real-time processing features afforded by this mode. This includes serialization, effective management of large and small message support for diverse modes of embedded networking solutions. It is also important to recognize that well tested implementations of this mode are readily available in computer languages, e.g. by Oracle/Java Crypto library. In other words, the market is waiting.

Avygdor Moise
Future DOS R&D Inc.

William L. Foster II

To whom it may concern,

I would favor a NIST review of EAX' for approval.

EAX' is a faster, low memory authentication when used with AES in place of CCM in wireless or embedded applications.
It can be streamed and handle messages of arbitrary length.

Additionally, it seems to be superior in M2M. Here is a IMECS 2011 quote from white paper analysis of M2M encryption/authentication comparing AES EAX and AES CMAC+CTR at iaeng.org by Bao Guo and William Yu.

"It is interesting to note that, AES EAX performs significantly better in splitting before encryption cases than AES CMAC+CTR.

This makes AES EAX better in streaming or online use cases. Considering AES-EAX performs similarly than AES

CMAC+CTR in ES cases but better in SE use cases, and that AES-EAX provides more security guarantees [12] we

suggest it be used for SMS-based data transport."

As a NIST CSWG, Standards subgroup member, it seems reasonable to give EAX, a non patented, proven secure scheme, the benefit a full review for approval.

Best regards,

William L. Foster II
CEO

Travis Mooney

To whom it may concern,

My name is Travis Mooney, and I am Schweitzer Engineering Laboratories' representative on ANSI C12 Main. SEL would like to abstain from comment on C12.22 because we do not intend to utilize the protocol in our meters.

Best Regards,
Travis

David R. Scott

Hi NIST,
As a voting member of the ANSI C12 Main Committee, I strongly support the “EAX’ mode in the ANSI C12.22 standard. The ANSI C12.22 Protocol Specification for Interfacing to Data Communication Networks [1] utilizes the EAX’ (EAX-prime) Cipher Mode. The motivation for this work was the somewhat unique requirements of supervisory control and data acquisition (SCADA) messaging associated with Automated Meter Reading (AMR) that operate in the context of an Advanced Metering Infrastructure (AMI), the principle use of this standard. However, these unique requirements may be applicable to many small embedded devices communicating in SCADA environments.

Thank you,

David R. Scott
Senior Project Manager | Energy Consulting & Engineering
SAIC Energy, Environment & Infrastructure, LLC

Tom Phinney

Subject: Comments on the NIST document: EAX' Cipher Mode (May 2011)

Disclaimer: I was the author of this variant of the EAX mode. I created it upon request of the ANSI C12 team that was attempting to fix the authenticated encryption then used in the ANSI C12.22 standard, which was rendered completely useless (i.e., trivially breakable) during the previous attempt to upgrade that standard from use of DES to use of AES.

Background: The ANSI C12.22 standard is such that nonces used to secure inter-device communication are of long and varying size. The destination and source addressing components of secured APDUs (Application-layer protocol data units), which are two components of the nonce required to secure those APDUs, are multi-octet object identifier strings with no a-priori-imposed size constraint.

For any given equipment vendor, it is likely that the APDU titles generated by its products are of an approximately fixed size, but because an electricity distribution network (also sometimes called a 'smart grid') contains equipment from different vendors, there is no a priori determinable maximum size for the addressing information required to designate communication endpoints in two such devices. This has the important consequence that

1) The maximum size of a nonce that includes one or two such addresses cannot be predetermined when establishing a network, unless the set of all device vendors whose products will be permitted to connect to that network over its entire lifetime, and the maximum size of APDU titles that those devices will use, is known at the time that the network is established.

The ANSI C12.22 standard reduces the message sizes that such large APDU titles would impose on the address fields of APDUs by compressing those APDU titles before transmission, from their inherent absolute form (anchored at the United Nations as the root organization, with a sequence of descendent organization arcs dependent therefrom) to a form that is relativized to the intended receiving device(s). This has two important consequences:

2) The actual representation (as a series of octet) of the message that is transmitted by an originating device is altered by each relay that forwards the message from the originator to the intended receiver(s).
3) Any cryptographic protection that uses those addresses in protecting the message needs to use a canonical form of these addresses, rather than the usually much smaller octet strings found in the message as actually transmitted or received.

Both of the authenticated-encryption-with-associated-data (AEAD) modes currently approved by NIST in SP800-38C (CCM) and SP800-38D (GCM) are unable to provide protection for ANSI C12.22 APDUs. CCM requires its nonce to be 13 octets or less, yet due to consequences 2) and 3) any nonce that includes the ANSI C12.22 APDU addressing information must use a canonical form, and thus typically will exceed 30

octets in size. GCM, as standardized by NIST, requires a constant-size nonce, and thus that all employing devices be configured with an absolute upper bound on the size of all nonces, yet due to consequence 1) that upper bound is not stable for the life of the network and thus cannot be configured into the network when deployed.

Analysis similar to that above led the ANSI C12 crypto group to look for alternatives. It was realized that any use of either CCM or GCM would require a mechanism for pre-compressing the nonce formed from the C12.22 messaging. Since such compression could result in nonce duplication within the lifetime of the relevant key, the results of the compression must itself be unpredictable to an attacker, thus compressing the original large nonce to a smaller bounded-size 'essentially fresh' value that can be substituted for any smaller nonce required by the selected AEAD mode.

For such compression to be unpredictable to an attacker, even by one that can reasonably predict message contents (as is often possible in this application), the compression must itself be key-dependent. The result is the creation of a new compound mode, consisting of keyed compression of the original large, varying-size nonce, followed by use of either CCM or GCM. Once this was realized – that any acceptable solution to the problem inevitably involved a new mode – the search for alternatives was widened to consider other modes, and in particular those which had been submitted to NIST for potential approval. At this point another highly desired capability of the mode became a consideration.

The ANSI C12.22 standard is used for both very small messages, consisting of only dozens of octets, and for very large messages that can exceed 64 KiB octets in size. For such large messages, the sending device may have timing constraints that require it to encrypt the message and compute its MAC in segments, just before the transmission of each, and/or the receiving device may have timing constraints that require it to decrypt the message and compute its incremental authentication in segments. (An example of this is a large download file sent by a backend computer through a network attachment device, where the backend computer expects an end-to-end acknowledgment shortly after it has provided the last segment of the transferred file.) In consequence:

4) A cryptographic mode with "online" capability is needed, to support 'chunked' serial encryption and decryption.

Both CCM and GCM are unable to provide "online" capability as specified by 4). EAX, which supports nonces of varying size, also can be used in an "online" mode. Furthermore, it has a proof of correctness (provided that its usage requirements are not violated). Also, it requires no complex computations beyond that of the underlying block cipher (presumably AES in North America, and presumably something other than AES in China). This is in contrast to GCM, which requires Galois field multiplication of 128-bit values in addition to the block cipher.

Many, probably most, of the devices that implement ANSI C12.22 are very small, low-power devices, typically embedded in residential premises electric power meters and equipment connected to those meters. Current implementations of such devices use

microcontrollers with compact instructions, a very limited amount of RAM, and a moderate amount of non-volatile memory that can be rewritten only infrequently (e.g., with new firmware downloads). Network communication may be via power-line carrier or very-low-power spread-spectrum IEEE 802.15.4 radio.

EAX is a very attractive AEAD mode for use in this environment. In addition to a key, it takes as input three strings, each of arbitrary length that may differ from one invocation to another. EAX compresses each of these three strings by CMAC (as specified in SP800-38B), then uses the result of the first input string's compression as an essentially fresh value for encrypting/decrypting the second input string (using CTR mode as specified in SP800-38A). It also combines the results of all three input string compressions in computing the overall authenticating MAC value.

Although the EAX documentation conceptualizes the nonce as separate from, and possibly redundant with, the other information that is authenticated by the EAX mode, there is no significant functional difference between the compression of the first and third input strings. Thus any information that would be included in the third input string can be included instead in the first input string at no difference in computational cost, with the resultant value used both as the nonce for use in the subsequent CTR-mode encryption step and as input to the aggregate authentication operation.

The above observation led the ANSI C12 cryptographic team to question whether the third input component could be dropped entirely from the EAX computation. Trial implementations for the smart meter environment also led to questions of whether the amount of per-key state needed for efficient processing could be reduced, to better match the limited RAM and computational capabilities of typical smart meter controllers. This led directly to the EAX-prime mode (which is so named because EAX prime is a derivative of EAX, and the prime is the classical mathematical notation for a derivative).

Comments on the published document:

1. Reference [8] contains a typo; it specifies "NIST SP 800-38C" but describes GCM and GMAC and provides the URL for SP800-38D. Thus the specification should be of "NIST SP 800-38D".

Aaron F. Snyder

The evaluation of EAX' by NIST is a welcome result that follows the committed effort of those dedicated to providing secure communications for advanced metering infrastructure deployments. Those professionals evaluated existing algorithmic approaches and concluded that while beneficial, did not offer all that was thought required for their particular application.

The approval of this mode will allow those wishing to leverage the ANSI C12.22 standard to its fullest, while not limiting innovation in the security or communications domains as applied to the deployment of advanced metering technologies.

Best regards,
Aaron F. Snyder, Ph.D.
Principal Consultant
EnerNex

John Lilley and Stephen J. Mikovits

Marianne et al,

SDG&E believes that NIST's review to approve EAX' should be conducted. We anticipate that this algorithm may provide optimizations to our AMI solution that could be beneficial to our customers in the future. The EAX algorithm may also be beneficial, although it was not specifically mentioned in the announcement on June 21, 2011. We rely on NIST reviews to provide expert vetting of cryptographic algorithms during our purchasing, configuration, and maintenance processes.

Thank you for your continuing support and your consideration of this activity. Please feel free to contact us if you need more information.

Primary contact
John Lilley
Smart Grid Security Architect
SDG&E, a Sempra Energy utility

Secondary contact
Stephen J. Mikovits
Director – Information Security and IS Compliance
SDG&E and So Cal Gas, Sempra Energy utilities

Michael Garrison Stuber

As NIST is aware, EAX', an optimized variant of EAX, is used in the C12.22 standard for meter networking. While Itron does not currently use EAX', instead using NIST approved CBC-mode, we strongly support NIST examining and approving both EAX and EAX'. As Rogaway and Wagner have demonstrated in their paper (http://www.cs.ucdavis.edu/~rogaway/papers/ccm.pdf), EAX has a number of technical advantages over CCM. Both CCM and GCM can be weak when used with short authentication tags (http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/comments/CWC-GCM/Ferguson2.pdf), and Saarinen has shown that GCM suffers from issues with weak keys (http://fse2011.mat.dtu.dk/rump/Finding%20GCM%20weak%20keys.pdf)

As a provider of Smart Grid solutions, Itron would like to adopt EAX' as described in the C12.22 standard. Furthermore, we would like to be able to use EAX proper in a variety of software applications. Itron is one of the leading providers of smart meters in North America, with millions of devices deployed, and millions more under contract. EAX' would benefit our solutions and our customers by providing more efficient messaging, and allowing us to provide a fully standards compliant solution. Currently, in order to meet customer requirements that our cryptographic solutions be NIST approved, Itron must provide security extensions to the C12.22 standard.

We urge NIST to move ahead with review and approval of EAX. Thank you.

--
Michael Garrison Stuber
Office of the CTO
Engineering Advisor, Standards and Security
Itron, Inc

Avygdor Moise

It is not clear to the public whether the comments sought by NIST are in regard to the approval of the proposal to consider the "cipher mode of operation that is specified in Annex I of ANSI C12.22-2008", for NIST approval; or whether the comments should focus on the actual EAX' mode. i.e. if approved will it only result in a second phase by NIST to approve the actual EAX' mode?

The two issues are significantly different. If the subject matter of this announcement is the approval of the proposal to approve EAX', then NIST is really asking whether a choice of a security mode that is already referenced by balloted national and international standards (ANSI C12.22 and IEEE 1703) should be re-evaluated by NIST and the community at large. If this is the case, then NIST and the community large should have joined the standards balloting pools when this question was asked in 2008, have cast their vote when the standards were balloted. It is my opinion that it is not the responsibility of NIST, at any time, to make a determination on the relevancy of the EAX' mode, given that it is was already established in published standards, as a pre-condition for consideration by NIST. i.e. The relevancy has been already established, and the used of these standard has been already included in rulings and references by PUCs (e.g. PUC Texas, Pennsylvania PUC, etc.) and utilities (e.g. EEI/AEIC group, BC Hydro, Ontario Hydro, and many more).

This mode is only one of many possible security profiles that may and can be implemented by the ANSI C12.22 and IEEE 1703 that defined a Smart Grid AMI Network Framework. It is the default 'built-in' mode. Any comment in this context needs to also consider whether not the comment originated from a person that has significant pragmatic working knowledge of the ANSI C12.22 and IEEE 1703 standards, which has nothing to do with the strength of EAX'

The only relevant subject matter for consideration should be: (1) given that EAX' exists, and (2) given that it is referenced by national and international standards, and (3) given the assertion by experts that it is needed for the use in large variety of constrained network environments, and (4) given that it is in use, and (5) given that it is referenced; does the EAX' cipher mode have any known vulnerability, when used properly in a peer to peer relationship between two actors.

Note 1: EAX mode was submitted on October 3, 2003 to the attention of NIST in order to replace CCM as standard AEAD mode of operation, since CCM mode lacks some desirable attributes of EAX and is more complex.

Note 2: EAX' was first referenced by ANSI C12.22 in 2008.

Avygdor Moise
Future DOS R&D Inc.

Lawrence A. Barto

The optimized block-cipher mode offered by Mssrs. Moise, Beroset, Phinney, Burns presents enhancements to other known authenticated encryption modes. It overcomes identified shortcomings found in the NIST-standardized CCM mode and builds further on the EAX mode. It is intended to best support the implementation of messages found in typical Smart Grid devices such as meters, remote terminal units, intelligent electronic devices and a variety of embedded devices which may have limited memory/code space. Most notably it addresses some unique requirements of these devices when used in Smart Grid systems including Advanced Metering Infrastructure.

The simplification shown achieves a reduction in the amount of per-key-related storage requirements without any significant weakening of the cryptographic strength and resistance to attack including denial of service attacks. The approach to provide further simplification over EAX mode such as identifying specific alternative initial CMAC blocks rather than arbitrary values as shown in the EAX mode should be beneficial to the industry.

Overall, this cipher mode appears to best support the requirements outlined in implementing ANSI C12.22, Protocol Specification for Interfacing to Data Communications Networks and as a result should help promote the security, performance, and interoperability of Smart Grid devices and systems.

I respectfully request NIST to strongly consider approve the use of EAX' block cipher mode to support the Smart Grid development efforts as well as any implementations using the ANSI C12.22 standard.

Sincerely,

Lawrence A. Barto
Metering Services Engineering Manager
Georgia Power Company

Alexander Shulgin

Hi,
In response to comments request about EAX' block cipher mode of operation i would like to say that I have successfully implemented and tested the EAX' encryption module in my C12.22 applications and it has very strong encryption/authentication level and good performace.
Please move it to approved state.

Thanks,
Alexander Shulgin
Software Developer

Edward J. Beroset

My name is Edward J. Beroset. I am the Director of Technology and Standards for Elster Solutions. By way of background, I am an embedded systems engineer with over fourteen years of experience in electric metering and in smart metering solutions. I participate in numerous industry standards-setting organizations including serving as chairman of the committee on ANSI C12.22, The company I work for, Elster Solutions, LLC, has designed and manufactured utility meters for 175 years and is a world leader in Advanced Metering Infrastructure (AMI). Elster was the first to market with true two-way Advanced Metering Infrastructure. We pioneered radio-frequency mesh communications for smart meters; and we have manufactured 200 million meters worldwide in the last ten years, including 5 million two-way smart electric meters in North America. We are passionate about seeing the promise of the smart grid brought to reality.

We feel that the EAX' mode, as specified in ANSI C12.22 and used in electricity metering systems worldwide, is important for NIST to approve. Unlike CCM and GCM, the other currently approved AEAD modes, EAX' was uniquely designed for use within embedded systems with contrained power, memory and computational capability. This was done without sacrificing security. To assure the continued security of AMI in particular and smart grid in general, we think it is important for NIST to approve this encryption mode. The industry relies on NIST to approve appropriately secure encryption modes and views approved modes as being of much higher value and security than unapproved modes. For this reason, rejection of the EAX' would send the wrong

messsage to industry and would risk the fracturing the interoperability that we have so far achieved through the use of this mode.

David Haynes

Dear NIST,

Thank you for your efforts to protect our country with cryptography.

I'm writing you today regarding the proposed EAX' mode of operating AES-128 cryptography. A number of electricity meter vendors and AMI vendors have looked at this mode and found it to be potentially useful for use in protecting "the grid". It appears to offer certain benefits in terms of efficiency which can be particularly useful for computationally constrained devices.

We at Aclara PLS manufacture communication systems which serve the electric power industry. We do of course plan to use cryptography which is NIST recommended, and to that end, it would be nice if we could consider EAX' as one of our options.

If time and budget permit, I ask that you take a look at EAX' to determine if it is indeed worthy of consideration for use in our industry.

Thanks,

David Haynes
Staff Systems Scientist

--

DCSI is now Aclara Power-Line Systems Inc

Richard D. Tucker

Dear Sirs:

I strongly support an acceptance of the EAX mode that has been upon the consideration and study of NIST and other groups interested in a strong and applicable security mechanism for our Smart Grid AMI Network.
Although ANSI C12.22 and IEEE 1703 allow many possible security profiles that may and can be implemented, a huge amount of time was spent with security experts' who recommended the EAX mode for those communications Standards that support the Electric Industry metering and Distribution data modeling of ANSI C12.19. As it turned out, the EAX mode was highly recommended and became the default 'built-in' mode for ANSI C12.22/IEEE 1703 in 2008.

Thank you for your consideration of my comment of endorsement of the EAX mode for our Smart Grid AMI Network.

Sincerely,

Richard D. Tucker, PE

Tucker Engineering Associates, Inc.
P.O. Box 326
Locust, NC 28097

Tyler Ivanco

To whom it may concern:

In my estimation, EAX' mode is essential for the Smart Grid and ANSI C12.22. Please move on with the approval process.

Kind Regards,

Tyler Ivanco, PhD

Thomas Herbst

It was recently brought to my attention that NIST is accepting comments regarding the use of EAX prime, especially as it relates to its use in ANSI C12.22.

For background, Silver Spring Networks (SSN) is a smart grid company, deploying AMI and DA networks. SSN has deployed AMI projects including 8 million networked meters. SSN has been awarded contracts to deploy more than 17 million meters.

None of the current or planned SSN deployments utilize C12.22 or EAX prime. Existing NIST approved modes are acceptable for smart grid and AMI deployment and approval of EAX prime is not necessary.

I am unaware of deployments by any vendor that implements C12.22 to the meter.

Thomas Herbst
Senior Director, Standards & Technology
Silver Spring Networks