From: Kelsey, John M. (Fed)
To: (b) (6)
Subject: FW: Rump session slides, Rene and John take over
Date: Tuesday, August 22, 2017 8:07:06 PM
Attachments: PQC, LWC, TDEA, 56A.pptx

From: "Peralta, Rene (Fed)" <rene.peralta@nist.gov>
Date: Monday, August 21, 2017 at 2:52 PM
To: "Chen, Lily (Fed)" <lily.chen@nist.gov>, "Barker, Elaine B. (Fed)" <elaine.barker@nist.gov>, "Mouha, Nicky W. (IntlAssoc)" <nicky.mouha@nist.gov>
Cc: "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>, "Dang, Quynh (Fed)" <quynh.dang@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Sonmez Turan, Meltem (Assoc)" <meltem.turan@nist.gov>, "Calik, Cagdas (IntlAssoc)" <cagdas.calik@nist.gov>, "Brandao, Luis (IntlAssoc)" <luis.brandao@nist.gov>, "McKay, Kerry A. (Fed)" <kerry.mckay@nist.gov>, "Regenscheid, Andrew (Fed)" <andrew.regenscheid@nist.gov>, "Dworkin, Morris J. (Fed)" <morris.dworkin@nist.gov>, "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Subject: Re: Rump session slides, Rene and John take over

I am attaching the finished slides. Send me any edits you wished done.

Rene.

From: Chen, Lily (Fed)
Sent: Thursday, August 17, 2017 10:40 AM
To: Peralta, Rene (Fed); Barker, Elaine B. (Fed); Mouha, Nicky W. (IntlAssoc)
Cc: Kelsey, John M. (Fed); Dang, Quynh (Fed); Perlner, Ray (Fed); Alperin-Sheriff, Jacob (Fed); Sonmez Turan, Meltem (Assoc); Calik, Cagdas (IntlAssoc); Brandao, Luis (IntlAssoc); McKay, Kerry A. (Fed); Regenscheid, Andrew (Fed); Dworkin, Morris J. (Fed); Moody, Dustin (Fed)
Subject: Rump session slides, Rene and John take over

Hi, Rene and John,

Attached is what collected, 7 slides (cover not counted). Because beacon slide is still blank, you two take over for the actions below.

1. Fill Beacon slide;
2. Do a dry run;

3. Figure out who will be the lucky presenter or both or just flyer;
4. Reformat, re-title, re-wording, do anything you like;
5. If we will talk at rump session, register it by noon next Monday or whenever before the deadline.
6. If we do flyers, print and bring to Crypto (This has to be done by Rene, John is not in the office).

Thank you, every one for providing the slides.

Lily

From: Peralta, Rene (Fed)
Sent: Wednesday, August 16, 2017 3:38 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Barker, Elaine B. (Fed) <elaine.barker@nist.gov>; Mouha, Nicky W. (IntlAssoc) <nicky.mouha@nist.gov>
Cc: Kelsey, John M. (Fed) <john.kelsey@nist.gov>; Dang, Quynh (Fed) <quynh.dang@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>; Calik, Cagdas (IntlAssoc) <cagdas.calik@nist.gov>; Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>; McKay, Kerry A. (Fed) <kerry.mckay@nist.gov>; Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Slides for TDEA and 800-56

Let's do a dry run, and time it.

Rene.

From: Chen, Lily (Fed)
Sent: Wednesday, August 16, 2017 3:34 PM
To: Peralta, Rene (Fed); Barker, Elaine B. (Fed); Mouha, Nicky W. (IntlAssoc)
Cc: Kelsey, John M. (Fed); Dang, Quynh (Fed); Perlner, Ray (Fed); Alperin-Sheriff, Jacob (Fed); Sonmez Turan, Meltem (Assoc); Calik, Cagdas (IntlAssoc); Brandao, Luis (IntlAssoc); McKay, Kerry A. (Fed); Regenscheid, Andrew (Fed); Dworkin, Morris J. (Fed); Moody, Dustin (Fed)
Subject: RE: Slides for TDEA and 800-56

Now we have about 7 slides (PQC(2), LWC(2), TDEA+56A/C(2) Beacon (1)). Can we handle 7 slides in 5 minutes? We are calling for “lucky presenter”?

Thanks,

Lily

From: Peralta, Rene (Fed)
Sent: Wednesday, August 16, 2017 2:46 PM
To: Barker, Elaine B. (Fed) <elaine.barker@nist.gov>; Mouha, Nicky W. (IntlAssoc) <nicky.mouha@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>
Cc: Kelsey, John M. (Fed) <john.kelsey@nist.gov>; Dang, Quynh (Fed) <quynh.dang@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>; Calik, Cagdas (IntlAssoc) <cagdas.calik@nist.gov>; Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>; McKay, Kerry A. (Fed) <kerry.mckay@nist.gov>; Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Slides for TDEA and 800-56

The Beacon stuff will just be one slide with a couple of bullet points.

Rene.

From: Barker, Elaine B. (Fed)
Sent: Wednesday, August 16, 2017 10:38 AM
To: Mouha, Nicky W. (IntlAssoc); Chen, Lily (Fed)
Cc: Peralta, Rene (Fed); Kelsey, John M. (Fed); Dang, Quynh (Fed); Perlner, Ray (Fed); Alperin-Sheriff, Jacob (Fed); Sonmez Turan, Meltem (Assoc); Calik, Cagdas (IntlAssoc); Brandao, Luis (IntlAssoc); McKay, Kerry A. (Fed); Regenscheid, Andrew (Fed); Dworkin, Morris J. (Fed); Moody, Dustin (Fed)
Subject: Slides for TDEA and 800-56

I put Nikky's TDEA info on one slide, and the 56A/C info on a second slide. Looks busy, but reduces the number of slides.

Elaine

From: "Mouha, Nicky W. (IntlAssoc)" <nicky.mouha@nist.gov>
Date: Monday, August 14, 2017 at 5:50 PM
To: "Chen, Lily" <lily.chen@nist.gov>
Cc: "'rene. gov'" <rene.peralta@nist.gov>, John Kelsey <john.kelsey@nist.gov>, Quynh <quynh.dang@nist.gov>, Ray Perlner <ray.perlner@nist.gov>, "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, Meltem Turan <meltem.turan@nist.gov>, "Calik, Cagdas

(IntlAssoc)" <cagdas.calik@nist.gov>, "Brandao, Luis (IntlAssoc)" <luis.brandao@nist.gov>, "McKay, Kerry A. (Fed)" <kerry.mckay@nist.gov>, Andrew <andrew.regenscheid@nist.gov>, Morris Dworkin <morris.dworkin@nist.gov>, "Elaine. Gov" <elaine.barker@nist.gov>, "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Subject: Re: Any updates we like to announce at crypto 2017?

http://csrc.nist.gov/publications/PubsSPs.html

NIST Special Publications - NIST Computer Security ...

csrc.nist.gov

Recommended Security Controls for Federal Information Systems has a similar scope to ISO/IEC 27002 and cross-references the standard.

PQC, LWC, TDEA, 56A/C, and Beacon

CRYPTOGRAPHIC TECHNOLOGY GROUP
COMPUTER SECURITY DIVISION
NIST

- POST-QUANTUM CRYPTOGRAPHY
- LIGHTWEIGHT CRYPTOGRAPHY
- 3 KEY TRIPLE DES (TDEA)
- SP 800-56A AND 56C
- NIST BEACON

The NIST PQC Standardization Project

NIST is calling for quantum-resistant cryptographic algorithms for new public-key crypto standards

- Digital Signatures
- Public-key encryption
- Key establishment (KEMs)

We may pick one (or more) of each type for standardization

Deadline for submission: November 30, 2017

Timeline	
Nov. 30, 2017	Submission deadline
April 2018	Workshop – Submitters' presentations (co-located with PQCrypto)
3-5 years	Analysis phase - NIST reports on findings and more workshops/conferences
2 years later	Draft standards available for public comments

- Submissions received by Sep. 30 will be reviewed for completeness, and we will notify the submitters of any deficiencies by the end of October
- 2 rounds of evaluation (12-18 months each)
  - Possible 3rd round, if needed
- See www.nist.gov/pqcrypto for full details
  - Sign up for the pqc-forum for announcements and discussion

NIST Lightweight Crypto Project

Plan

Develop and maintain a portfolio of lightweight algorithms that are intended for limited use.

Each algorithm will target one or more *profiles*, which consists of algorithm goals, acceptable ranges for metrics, limitations.

Draft Profiles

Profile I AEAD and hashing for constrained software and hardware environments.

Profile II AEAD for constrained hardware environments.

Contact

Mailing list: lwc-forum@nist.gov

Webpage: https://www.nist.gov/programs-projects/lightweight-cryptography

References

1. NISTIR 8114: Report on Lightweight Cryptography
2. Draft White Paper - Profiles for the Lightweight Cryptography Standardization Process

Comments Requested on TDEA

Update to Current Use and Deprecation of TDEA: (see http://csrc.nist.gov/news_events/)

- Plans: Decrease data limit per key bundle

  Disallow TDEA for some protocols (e.g., TLS)

  Develop deprecation timeline

-Send comments to TDEA_Deprecation@nist.gov by Oct. 1

SP 800-67 Rev. 2: (see http://csrc.nist.gov/publications/PubsSPs.html)

- New data limit to apply protection (e.g., encrypt) per key bundle:

  Old limit: 2^{32} blocks; New limit: 2^{20} blocks

- Send comments to SP800-67comments@nist.gov by Oct. 2

Comments Requested on SP 800-56A and 56C

(Available at http://csrc.nist.gov/publications/PubsSPs.html)

SP 800-56A Rev. 3

- FFC: Use specific safe-prime groups (GF(p), p = 2q+1)
- ECC: Use commonly used curves
  - Key derivation methods (KDMs) moved to SP 800-56C
  - Send comments to SP800-56a_comments@nist.gov by Nov. 6

SP 800-56C Rev. 1

- All KDMs now included for SP 800-56A and B
- KMAC128 and KMAC256 included for single-step KDMs
  - Send comments to SP800-56C_Comments@nist.gov by Nov. 6

The NIST Beacon
(available at https://beacon.nist.gov/home)

- Production version will be deployed in a few weeks.

- The new API will have support for combining beacons.

- Univ. of Chile, IBM are planning to deploy their own beacons.