From: Chen, Lily (Fed)
To: Brandao, Luis (IntlAssoc)
Subject: RE: Poster/Presentation on SDO-Collaborations wrt NIST-Crypto Standards
Date: Sunday, October 24, 2021 10:54:00 PM

Hi, Luis,

I think the current version is good to go. Thanks,

One thing I like to clarify. We consider ISO as "International Standards Organization" because, its members are "National Bodies (NBs)". Each NB votes for approval or disapproval. An ISO standard may specify multiple algorithms, submitted by different countries. NIST hasn't standardized an algorithm because it is in an ISO standard. For example, SM3 is a hash function submitted by China. It is specified in ISO/IEC 10118-3 together with SHA2 and SHA3. This is what I mean that NIST usually does not adopt international standards.

We consider IEEE 802 as a standards organization for a specific industry, even though it has individual members from different countries. Each individual is a voter if the individual attended more than 3 meetings per year. For example, Cisco implement IEEE 802.11 protocols in their wireless routers. The routers can be used by government. NIST adopts KDFs so that the router can get FIPS 140 validated.

The same for IETF even though IETF has no formal ballot. IETF has international participants. But we consider IETF is specifically for Internet protocols.

X9 is also member-based. NIST is a X9F member. Most of the members are banks. It has different level of membership with different fees. X9F1 is one of the earliest adopters of public-key cryptography. NIST standards, SP 800-56A and SP 800-56B are mainly adopted X9 standards. But X9F1 has not been active in the past 10 years, because, instead of developing bankers' specific crypto standards, the banks also use IETF protocols with NIST crypto standards.

If you have further questions, please let me know.

Lily

From: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>
Sent: Sunday, October 24, 2021 7:01 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: Poster/Presentation on SDO-Collaborations wrt NIST-Crypto Standards

Thanks Lily,

Improved version attached. The notes below explain the new edits and reflect on your comments.

I'll submit an updated poster this Monday morning to the SciencDay team (they still have the version from the past week), but am also open to do further improvements till the actual oral presentations, in case you have more feedback.

========== In column 1

Within the space constraints, made some changes (A, below) that should clarify things, aligned with your comments. Still have a doubt about one of your comments (C, below).

====== A. Did the following changes:

- A0. Before the rectangle "NIST <--> SDOs", added a note [improves ...] "U.S. competitiveness in the global marketplace"

- A1. 1st bullet (the previous was "<B1>. <B2>", below) improved to "SDOs adopt NIST crypto standards. Thus, vendors with products using NIST standards to meet U.S. Gov. needs can also enter Int'l markets.

- A2. 2nd bullet (the previous was "<B3>. <B4>", below) improved to "NIST adopts SDO's best-practice standards. Thus, vendors in some industries get abler to operate in settings requiring NIST-approved standards."

====== B. Previous version (for comparison)
In the previous version the two bullets, each with a <Title with direction of assimilation> and a <benefit explanation>, were as follows:
- B1. 1st bullet title: "SDOs incorporate NIST crypto standards."
- B2. 1st bullet explanation: "International contexts required to follow other SDOs will benefit from NIST developed standards."
- B3. 2nd bullet title: "NIST incorporates SDO's standards."
- B4. 2nd bullet explanation: "Vendors that must follow NIST-approved crypto standards benefit from standards originating from other SDOs"

====== C. Clarification question:

- C1. You mentioned [We do not usually adopt international standards.]. I understand that adoption of Int's standards may not be the default, but, for example:
  - Isn't the IETF EdDSA a case of an adopted International standard?
  - [unless I misinterpreted a comment in an earlier email] Weren't the KDFs in NIST SP 800-108 adopted from IEEE 802.11?

- C2. It wasn't clear to me if you intended to suggest that the title of the 2nd bullet (B3) should change, or if this was just to highlight that the NIST's adoption of SDO's standards is only in very focused cases of industry/application best-practices. The new version (A2) may at least already have improved a bit compared to the previous one.

====== D. Generic comments about types of SDO

- D1. I think there's not much space in this poster to differentiate between industry-or-app-specific vs. generic SDOs, and U.S.-only vs International SDOs, but:
  - Some of these (and the various comments in the previous emails) can be mentioned in the oral presentation;
  - The more thorough future presentation can explain various of these aspects. Will consider adding a new slide (e.g., explaining the types of SDO's and how the motivate various types of interactions) to the draft structure.

- D2. Would you find correct to say that, wrt standards development, X9 is national (U.S.) [even though the developed standards affect the world], whereas ISO, IEC, TCG, IETF and IEEE are International?

- D3. Note: in the ANSI (dot) org website I find SDO-explanation links to all except TCG. https://webstore.ansi.org/sdo/nist (e.g., replace nist by ieee, nsit, iec, iso, x9)

========== In column 3:

====== E. In the "Looking forward" section

- E1. 2nd bullet: Small tweak to the text.

- E2. 3rd bullet: About InfoSec vs. CyberSec, I agree any version would not be incorrect here. Based on intuition, left it as was.

I agree that the "software signing" application relates more directly to CyberSec, and I'd say that a standalone "signature scheme" (e.g., FIPS 186) standard relates more directly to InfoSec when it can be explained/motivated based on fundamental principles of integrity/authenticity of data (say, abstracting from the notion of software).

In summary, I think the distinction can sometimes be useful to differentiate between (i) [InfoSec] standards focused on fundamental building blocks related to principles of InfoSec, and (ii) [CyberSec] standards-or-guidance-or-practices that take advantage of those building blocks to enable security of higher-level applications (in Internet protocols, ...)

Regards, Luís

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Sunday, October 24, 2021 10:28
To: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>
Subject: RE: Poster/Presentation on SDO-Collaborations wrt NIST-Crypto Standards

Hi, Luis,

Thanks for improving the poster. I like you to present. It is going to be a brief presentation. Let's do not switch. You will do a great job. I am fine with all the changes.

About information security vs. cybersecurity, I am okay with either. Please note that software signing or code signing to prevent malware attacks may not be considered as information security but cyber security. Digital signature is used for code signing and also for root of trust.

The only place which I like to think more is in the first column.

- SDOs incorporate NIST crypto standards. International contexts required to follow other SDOs will benefit from NIST developed standards.
- NIST incorporates SDO's standards. Vendors that must follow NIST-approved crypto standards benefit from standards originating from other SDOs

SDOs are different.

1. For international SDOs like ISO, from one point of view, the vendors who have implemented NIST standards for US government usage need to enter international market. The vendors cannot do two versions of their products, one of them is only for government. This is a way to promote "U.S. competitiveness in the global marketplace". [We do not usually adopt international standards.]
2. For industry and application SDOs, there are two situations. When they adopt NIST cryptographic standards, the products complying those standards can get FIPS 140 validated and can be used for government. Another situation is that NIST adopts the standards developed in those SDOs as industry best practice. The purpose is also for government usage.

I am concerned the statements above not precisely reflect these situations.

Lily

From: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>
Sent: Saturday, October 23, 2021 3:27 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: Poster/Presentation on SDO-Collaborations wrt NIST-Crypto Standards

Hi Lily,

Thank you for the feedback and confirmation. On Monday early morning I should send to the SciDay team the new poster and let them know the presenters. May I inform them that we'll jointly present (if you are available)?

Below is a list of the new editorial improvements, implemented in the newly attached version (PDF).

Please note in particular the three cases preceded with "PLEASE CHECK". I'm fine with reverting back / or adapting more any item, if you have any additional feedback.

=== A. All columns --- removed all occurrences of "e.g." (for a simpler looking poster):
- A1. 1st col, 1st par (before the cliparts): ", e.g.:" --> "."
- A2. 2nd col, 1st par: "needs a motivation (e.g., app. area)" --> "has a motivating application area"
- A3. 2nd col, IETF: "(e.g., TLP, IPsec, ...)" --> "(TLP, IPsec, ...)"
- A4. 3rd col, 1st bullet: "NIST standards (e.g., PQC, LWC)" --> "NIST PQC and LWC standards"
- A5. 3rd col, 2nd bullet: "(e.g., PEC, Threshold)." --> "such as PEC and Threshold."

=== B. 1st column:
- B1. 1st sentence: centered and avoiding hyphenation in the first line
- B2. 2nd bullet -- micro font-size reduction, to avoid hyphenation and allow avoiding abbreviation "stnds". Tweak: "from stnds developed in other SDOs." --> "from standards originating from other SDOs."
- B3. Win-win 1st bullet: "saving human resources" -> "enhancing resource efficiency"; "sharing of expertise" --> "sharing expertise";
- B4. Win-win 2nd bullet: "widely accessible" --> "producing widely accessible" [for uniformity with previous bullet]
- B5. improved footnote

=== C. 2nd Column:
- C1. (previous typo) TCB --> TCG
- C2. removed the "app" acronym (no longer needed)
- C3. **PLEASE CHECK:** Upon a new read, the sentence "CTG involved beyond crypto: security and protocols" gave me some pause, because crypto also includes considerations about security and protocols. I think the point is that the CTG involvement goes beyond "primitives". How about saying (implemented) "CTG deals with primitives, protocols and security" [carefully fitting within one line]?

=== D. 3rd column:
- D1. **PLEASE CHECK:** Is the statement/positioniong about the HomomorphicEncryption

collaboration accurate?
- D2. 1st bullet: "of NIST standards (e.g., PQC, LWC)" --> "of upcoming NIST PQC and LWC standards"
- D3. **PLEASE CHECK:** Incorporated your proposed change "Continue cutting-edge research and lead standards development for cybersecurity needs", but with two tweaks: added "crypto" before "standards"; changed "cybersecurity" to "information security" [this is a soft suggestion --- please see the comment further below *], resulting in "Continue cutting-edge research and lead crypto standards development for information security needs". Maybe yet another alternative [avoiding reflecting on info-sec. vs. cybersec.], inspired by the ISO-IEC/JTC1/SC27/WG2 title, would be to mention "Continue cutting-edge research and lead standards development for cryptography and security mechanisms."? Which of the three versions (or any alternative) would you prefer?
- D4. Improved line: "Find NIST crypto publications (FIPS, SP 800, etc.) at link ..."

*** Reflection note on cybersecurity vs. information security:**

I may be overthinking (or, rather, not yet reflected enough to come up with a strong conclusion), but in some cases related to crypto standards I think that "information security" provides a better context/connotation than "cybersecurity".

I was just recently looking at how to interpret "cybersecurity", to understand the possible different connotations associated with the titles of the CSD and ASD divisions, and also when thinking how to position the PEC work. That lead me to consider the differentiation between "cybersecurity" and "information security", where the latter (InfoSec) seems somewhat more fundamental (i.e., in line with crypto standards), whereas the former (cybersecurity) would be more applied (e.g., including software vulnerabilities, risk mitigation, etc.). I concede that this interpretation is somewhat intuitive and flexible. (For example, TLS could be well associated with cybersecurity.)

As an example, on a quick Google search for "cybersecurity vs information security", the first result https://analyticsindiamag.com/difference-between-cybersecurity-information-security/" mentions:

"Cybersecurity usually deals with cybercrimes, cyber frauds and law enforcement. On the contrary, information security deals with unauthorised access, disclosure modification and disruption.

Cybersecurity is handled by professionals who are trained to deal with advanced persistent threats (APT) specifically. Information security, on the other hand, lays the foundation of data security and are trained to prioritise resources first before eradicating the threats or attacks."

Regards, Luís

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Saturday, October 23, 2021 09:17
To: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>
Subject: RE: Poster/Presentation on SDO-Collaborations wrt NIST-Crypto Standards

Hi, Luis,

Thanks for continuing to improve the poster. I like the attached version better. By another try, I mean another pass to work on the poster. We definitely will present it. Hopefully, we can get some useful feedback so that we can identify some focus point for SDO participation. Here are a few comments/suggestions/questions to consider.

Column 1: Change "saving human resources" to "enhancing resource efficiency".
Column 2: After TCG, what TCB stands for?
Column 2: "CTG only participates in selected sub-committees" sounds not positive enough. How about "CTG participates in with well justified priorities" or something similar.
Column 3: The sentence "Besides crypto standards, will also continue developing crypto research and applications" can be tweaked a little and remain focused on standards. How about "Continue cutting-edge research and lead standards development for cybersecurity needs"?

Thanks.
Lily

From: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>
Sent: Friday, October 22, 2021 7:47 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: Poster/Presentation on SDO-Collaborations wrt NIST-Crypto Standards

Now attaching a better version with a few corrections.

From: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>
Sent: Friday, October 22, 2021 19:00
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: Poster/Presentation on SDO-Collaborations wrt NIST-Crypto Standards

Hi Lily,

Thank you for the additional feedback!

I made significant corresponding updates in the poster, described further below. Notably, the

poster no longer enters into details about each SDO, but instead just identifies the sub-committes or the context area for each. Thus, the spirit is no longer about detailing standards in each SDO, but more about conveying that CTG has a wide range of interactions with several SDOs.

Clarification question: by "Let's give another try", did you mean (i) doing an improvement to the poster to get better, to still consider the Science Day, or (ii) leave it for another time and not present at this year's Science Day?

If you feel that the poster --- attached* --- is good for a presentation at the Science Day, would you be interested in co-presenting it (or present it, if you prefer)?

* 'm open to continue improving based on possible further feedback/suggestions.

Updates since the previous version:

=== Column 1:
- Better direct focus on the CTG
- Added cliparts (visual spirit requested for SciDay) about what CTG standardizes; less text.
- Improved text overall (and more bulletized)

=== Column 2:
- New initial conveying that interactions and impact vary with the app. area, and require a motivation to justify resources.
- New table: allowing much less text. Emphasizes the sub-committees / context (easier to understand). No longer depends on the concrete context (to be covered in crypto-club panel).
- Some new bullet notes based on your feedback

=== Column 3:
- Simpler text about ZKProof
- Revised text about "Looking forward"
- Shorter legend. New space for links to CTG group and CRSC pubs.

Regards, Luís

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Friday, October 22, 2021 14:42
To: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>
Subject: RE: Poster/Presentation on SDO-Collaborations wrt NIST-Crypto Standards

Luis,

Thank you for the effort to create the poster for Science Day. By nature, it is not easy to put so many different topics in one poster and let people walk away with something impressed. For each of the standard organizations (or most of the cases, a sub-committee and a sub-group) there is a story to tell and a background to justify the resource we have used. Let's give another try.

B3: ISO/IEC includes a lot committees, CTG only worked in ISO/IEC JTC1 SC27 WG2 - Cryptography and security mechanisms. In WG2, there are more than 20 active projects. We contributed the projects which are related to NIST Cryptographic Standards.

IEEE-SA is NOT for WiFi. IEEE-SA includes tons of standards projects. IEEE 802 is for local area networks (LAN), personal area network (PAN), and metropolitan area networks (MAN). What we contributed is 802.11 (which is WiFi).

Also please notice that CTG involvements to the standards are not only for cryptography. It can be related to security protocols, interoperability, etc.

C: We can say some high level future plan such as promote adoptions of NIST cryptographic standards in different application environment and international standards. But I do not think it should be specific to each organizations.

We can talk about presentations in reading club late.

Lily

From: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>
Sent: Friday, October 22, 2021 8:45 AM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Poster/Presentation on SDO-Collaborations wrt NIST-Crypto Standards

Hi Lily,

Two notes below:
- 1. Poster for sci-day?
- 2. Future presentation for the reading club?

====== 1. Poster?

The poster submission was accepted for SciDay, but as mentioned I'd like to leave to your discretion whether or not you think this should/can be presented. I can still update it or retract it. Besides the 10 min of presentation during sciday, the benefit that I find is to have this be a summary with context about crypto standards activities, in complement to the posters of the two previous years (2019 and 2020). It also motivates a subsequent crypto

reading club presentation.

The current poster version is here: poster-standards-collab

In any case, even before SciDay I'd still like to improve the visual look and info (reduce the running text) as follows:

(I'd especially benefit from some input/feedback about items B3, B4 and C)

== B. In the 2nd column:

- **B1.** Reorganize some of info into a table (logo / sub-committe / example application area), and then follow with some bullet points (with less running text).

- **B2.** Remove the somewhat redundant repetition (e.g., across ISO/IEC, X9, IETF) that the (more-or-less) same NIST standards (e.g., AES, SHA, key agreement, signatures) have been adopted. Find a way to just mention these NIST standards once (and possibly add some cliparts about the primitives).

- **B3.** About ISO/IEC: Any suggestion of is one or some areas of stakeholders/applications of ISO/IEC crypto standards? Note that we already have areas identified for the other SDOs, e.g., IETF --> Internet protocols; X9 --> financial sector; IEEE-SA --> WiFi.

- **B4.** About TCG / root of trust: Any suggestion for an additional sentence of content/context?

== **C.** In the 3rd column, section "Looking forward" (intended to mean "conceivable future activities"), do you think the bullet points are valid/clear?
- 1st bullet: While I don't known of any concrete plan, I just assume here that various SDOs will want to approve NIST PQC and LWC standards once they are defined. Is this reasonable?
- 2nd bullet: retrieved it from one of your bullet points about ISO. Does this seem to convey a reasonable idea in general?

Any other comment is of course also welcome about any column.

====== 2. Future presentation?

To take advantage of the notes you have provided so far, as well as the replies fromQuynh and Elaine, I add them all into a draft slide-deck, with various place-holders for more content.

A link to a viewable PDF (does not require overleaf account) is here:

https://www.overleaf.com/read/crnzjcgtkqwk
(It takes a few seconds to compile, once opening)

Would this be a starting point in the right direction for a possible future NIST-internal crypto reading club talk (perhaps for December or January), to present/discuss information more thorough than in the poster? I'd imagine trying to jointly build a clean presentation perhaps in the span of a couple of months.

Thank you in advance for any comment.
Regards, Luís