A Lightweight Talk on Cryptographic Standardization at ISO

Orr Dunkelman

In cooperation with so many people: Tomer Ashur, Atul Luykx, *********, **********, …

אוניברסיטת חיפה
University of Haifa
جامعة حيفا

ISO 3103

- Defines the process of brewing a tea cup

אוניברסיטת חיפה
University of Haifa
جامعة حيفا

ISO 4165

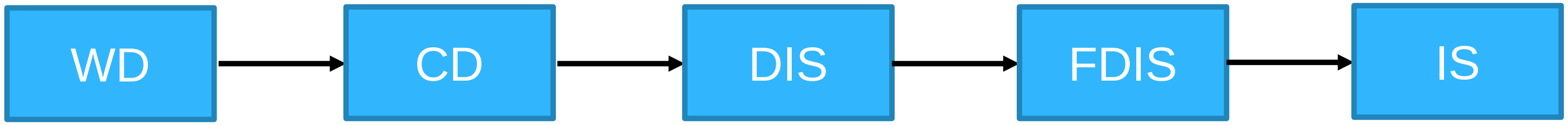
- Defines the power outlets of cars

International Standardization Organization

- Covers different types of standards
- Divided into different committees
  - we discuss ISO/IEC JTC 1 (ICT technologies)
- Committees are further divided into subcommittees:
  - SC27 – IT Security Techniques
  - SC31 – Automatic identification and data capture techniques
  - SC37 – Biometrics
- Subcommittees are further divided into working groups:
  - SC27/WG2 – Cryptography and security mechanisms
  - SC27/WG3 – Security evaluation, testing and specification
  - SC31/WG4 – Radio communications (RFID, RTLS, Security)

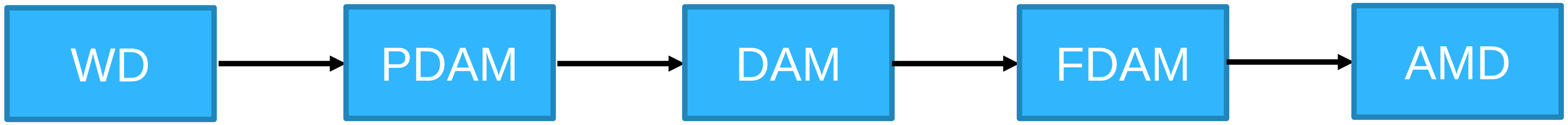
The ISO Process (Simplified)

New Standard



WD → CD → DIS → FDIS → IS

Amending Standard



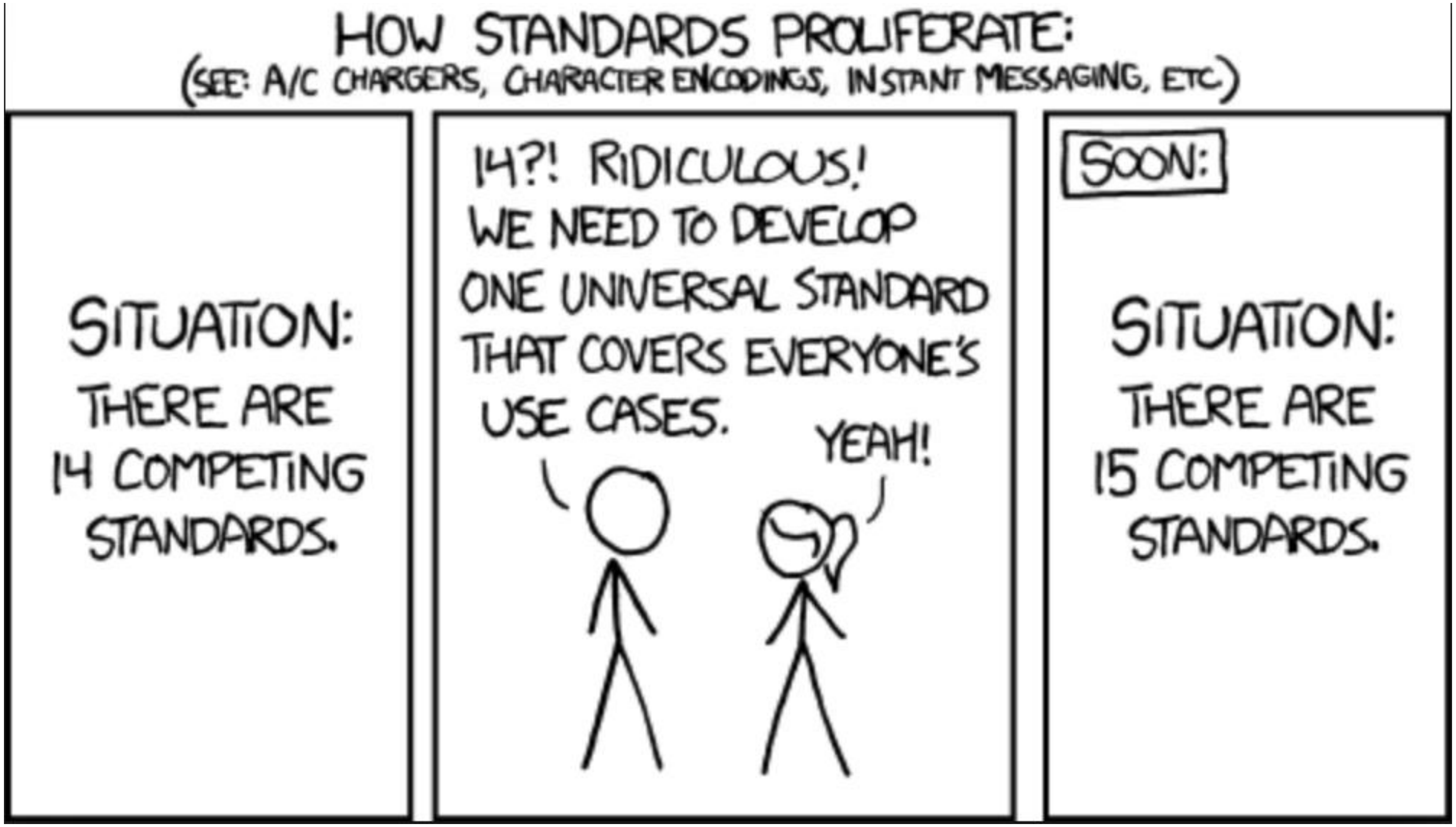
WD → PDAM → DAM → FDAM → AMD

Pre-Working Draft

- Preliminary:
  - Announcement
  - Study Period (Discussion)
  - Decision – Continue to Proposal/Go back to SP/Cancel
- Proposal:
  - Registration
  - Vote
  - Study Period + Improvements
  - Decision – Continue to WD/Go back to SP/Cancel

- See codes at https://www.iso.org/stage-codes.html

Cryptographic Standardization


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

“The good thing about standards is that there are so many to choose from” — Andrew S. Tanenbaum

אוניברסיטת חיפה
University of Haifa
جامعة حيفا

Cryptographic Standards of ISO

- Offer multiple options for the same task
- ISO 9797-1 (Block Cipher-based MACs):
  - Defines 6(!) different approaches for using an n-bit block cipher to produce m-bit tag
  - 3 different paddings, 2 different initial transformations, 3 different output transformation
  - + Truncation! (rightmost bits)
  - Alg. 1: CBC-MAC
  - Alg. 5: CMAC
  - For more details – purchase ISO 9797-1:2011 for just 158 CHF

אוניברסיטת חיפה
University of Haifa
جامعة حيفا

Cryptographic Standards of ISO

- ISO 9796: Signatures with message recovery
- ISO 9797: MACs
- ISO 9798: Security Authentication
- ISO 18033-2: Asymmetric encryption
- ISO 18033-3: Block ciphers: 3DES, Misty1, CAST128, HIGHT, AES, Camellia, SEED
- ISO 18033-4: Stream ciphers
- ISO 10118: Hash Functions: SHA224, RIPEMD128, RIPEMD160, SHA1, SHA256, SHA384, SHA512, Whirlpool
- ...

אוניברסיטת חיפה
University of Haifa
جامعة حيفا

Lightweight Cryptography (ISO 29192)

- 29192-2: Block ciphers: PRESENT, CLEFIA
- 29192-3: Stream ciphers: Enocoro, Trivium
- 29192-4: Asymmetric
- 29192-5: Hash functions: Photon, SpongeNT, Lesamnta-LW

The ISO 18031 Fiasco

- A.K.A. Dual EC DBRG
- 2005: introduced
- June ‘06: ANSI SP 800-90A
- Crypto ‘07: Dan Shumow & Niels Fergueson – “It’s a point? It’s another point? It’s a backdoor!”
- 2013: Snowden revelations

אוניברסיטת חיפה
University of Haifa
جامعة حيفا

How ISO works

- Votes are done by country (NB)
- During the meeting (every 6 months), the WG can have as many experts representing a WG
- Votes then are “advisory”
- After the meeting of WG (and during the meeting), a HoD vote takes place
- After that HoD vote, a plenary of the SC takes place

Simon/Speck

- ARX design by the NSA
  - For the NSA?
- Received a great deal of cryptanalytic attention
- Submitted to standardization…

Recent Results

- Two weeks ago, SC27/WG2, voted for the cancelation of Simon&Speck as part of PDAM3: 8-4 (4 abstained)
- SC27 rectified this decision explicitly: 14-3 (8 abstrained)
- Wall of shame in SC27: US, UK, KR

- So Simon/Speck in SC27 is (currently) off the table!

But wait there is more!

- ISO SC31/WG4 is close to standardize these ciphers for RFID authentication (FDIS)
- How come they didn’t consult with SC27?
- No need!

אוניברסיטת חיפה
University of Haifa
جامعة حيفا

Your help is needed!

- Contact your NB
- Tell them to speak with the SC31/WG4 people
  - Option 1: Explain to them that standardization of weak crypto when SC27 rejected it is a bad idea, ask them to consult the SC27 experts
  - Option 2: Tell them that following SC27’s decision, you fear the security of the proposed FDIS. Ask them to increase number of rounds
  - Option 3: Participate in ISO! (and IETF, ETSI, IEC, NIST processes and more)

אוניברסיטת חיפה
University of Haifa
جامعة حيفا

Thank you for your attention!

מתי

THE STANDARDS INSTITUTION OF ISRAEL

אוניברסיטת חיפה

University of Haifa

جامعة حيفا