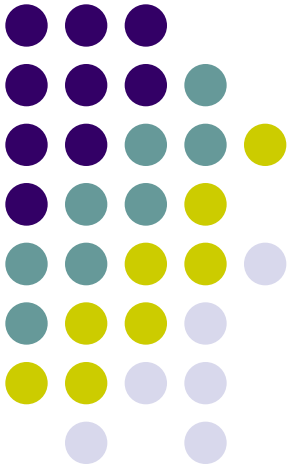
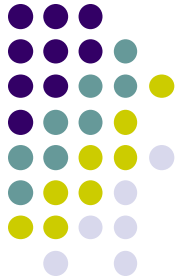
Introduction

Zdeněk Říha



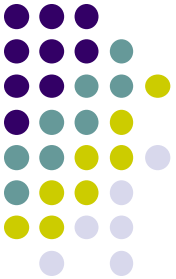
Why do we need standards in IT Security?



- Compatibility/interoperability
- Common terminology
- Efficiency/costs – no need to reinvent a wheel
- Regular updates/follow developments
- …

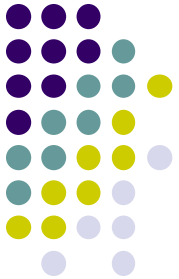
- Security

Disadvantages



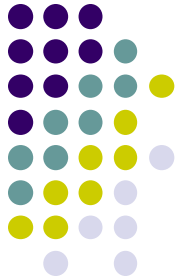
- Paid standards
  - To cover the development of standards
- Competition among the standardization bodies
- Access to standards (and their drafts)
  - + difficult to understand
- Reduced flexibility
  - E.g. for small organizations

Coverage



- From high-level management
  - ISMS (information security management system)
  - E.g. ISO 27000
- Up to low level crypto
  - E.g. RSA, PKCS#1

Standards vs. norms

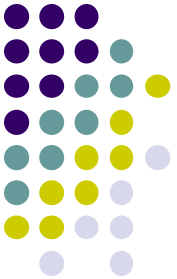


- Standards are recommendations
- Norms are authoritative (mandatory) standards
- Normativity depends on:
  - Country
  - Time
  - Field/context
  - Type of company, personal use/business use

Standardization bodies

- ISO
- National SO
  - Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, ČSN
  - UNMS SR (Slovakia)
  - DIN (Germany)
  - AFNOR (France)
  - ANSI (USA)
- CEN – European association
- CEN, CENELEC and ETSI - recognized as European Standards (ENs)

Standardization bodies



- NIST: National Institute of Standards and Technology (USA)
- ETSI European Telecommunications Standards Institute
- ITU-T (e.g. X.509)
- IETF – RFC

- RSA Security (PKCS)

Process

- The full list of status codes of ISO standards
- Focus on involvement of stakeholders, not on speed
- Often public consultations are needed

STAGE	SUBSTAGE						
				90 Decision			
	00 Registration	20 Start of main action	60 Completion of main action	92 Repeat an earlier phase	93 Repeat current phase	98 Abandon	99 Proceed
00 Preliminary stage	00.00 Proposal for new project received	00.20 Proposal for new project under review	00.60 Close of review			00.98 Proposal for new project abandoned	00.99 Approval to ballot proposal for new project
10 Proposal stage	10.00 Proposal for new project registered	10.20 New project ballot initiated	10.60 Close of voting	10.92 Proposal returned to submitter for further definition		10.98 New project rejected	10.99 Approval to New project approved
20 Preparatory stage	20.00 New project registered in TC/SC work programme	20.20 Working draft (WD) study initiated	20.60 Close of comment period			20.98 Project deleted	20.99 WD approved for registration as CD
30 Committee stage	30.00 Committee draft (CD) registered	30.20 CD study/ballot initiated	30.60 Close of voting/ comment period	30.92 CD referred back to Working Group		30.98 Project deleted	30.99 CD approved for registration as DIS
40 Enquiry stage	40.00 DIS registered	40.20 DIS ballot initiated: 12 weeks	40.60 Close of voting	40.92 Full report circulated: DIS referred back to TC or SC	40.93 Full report circulated: decision for new DIS ballot	40.98 Project deleted	40.99 Full report circulated: DIS approved for registration as FDIS
50 Approval stage	50.00 Final text received or FDIS registered for formal approval	50.20 Proof sent to secretariat or FDIS ballot initiated: 8 weeks	50.60 Close of voting. Proof returned by secretariat	50.92 FDIS or proof referred back to TC or SC		50.98 Project deleted	50.99 FDIS or proof approved for publication
60 Publication stage	60.00 International Standard under publication		60.60 International Standard published				
90 Review stage		90.20 International Standard under periodical review	90.60 Close of review	90.92 International Standard to be revised	90.93 International Standard confirmed		90.99 Withdrawal of International Standard proposed by TC or SC
95 Withdrawal stage		95.20 Withdrawal ballot initiated	95.60 Close of voting	95.92 Decision not to withdraw International Standard			95.99 Withdrawal of International Standard

Versioning (ISO)

ICS › 35 › 35.240 › 35.240.15

ISO/IEC 7816-4:2020

Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange

LIFE CYCLE

A standard is reviewed every 5 years

00 | 10 | 20 | 30 | 40 | 50 | **60.60** Publication | 90 | 95

REVISIONS / CORRIGENDA

Previously	Now
ISO/IEC 7816-4:2013	ISO/IEC 7816-4:2020
ISO/IEC 7816-4:2013/Amd 1:2018	
ISO/IEC 7816-4:2013/Cor 1:2014	
ISO/IEC 7816-4:2013/Amd 2:2018	

Versioning (RFCs)

- RSA Encryption

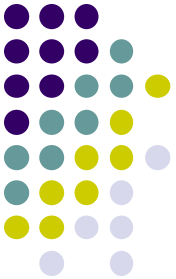
RFC 2315

RFC 2437

RFC 3447

RFC 8017

Versioning (NIST FIPS)



- Digital Signature Standard
  - FIPS 186 (published May 1994)
  - FIPS 186-1 (published Dec 1998)
  - FIPS 186-2 (published Jan 2000)
  - FIPS 186-3 (published Jun 2009)
  - FIPS 186-4 (published Jul 2013)
  - FIPS 186-5 (published Feb 2023)

Versioning

- PKCS#1 v1.5
- ETSI TS 119 312 V1.4.2 (2022-02)
- ITU-T X.509 Version/Edition

4	X.509 (03/2000)	Superseded
3.6	X.509 (1997) Technical Cor. 6 (04/2004)	Superseded
3.5	X.509 (1997) Technical Cor. 5 (02/2003)	Superseded
3.4	X.509 (1997) Technical Cor. 4 (04/2002)	Superseded
3.3	X.509 (1997) Technical Cor. 3 (10/2001)	Superseded
3.2	X.509 (1997) Technical Cor. 2 (02/2001)	Superseded
3.1	X.509 (1997) Technical Cor. 1 (03/2000)	Superseded
3	X.509 (08/1997)	Superseded
2	X.509 (11/1993)	Superseded
1	X.509 (11/1988)	Superseded

9	X.509 (10/2019)	In force
8	X.509 (10/2016)	Superseded
7.3	X.509 (2012) Cor. 3 (10/2016)	Superseded
7.2	X.509 (2012) Cor. 2 (04/2016)	Superseded
7.1	X.509 (2012) Cor. 1 (05/2015)	Superseded
7	X.509 (10/2012)	Superseded
6.3	X.509 (2008) Cor. 3 (10/2012)	Superseded
6.2	X.509 (2008) Cor. 2 (04/2012)	Superseded
6.1	X.509 (2008) Cor. 1 (02/2011)	Superseded
6	X.509 (11/2008)	Superseded