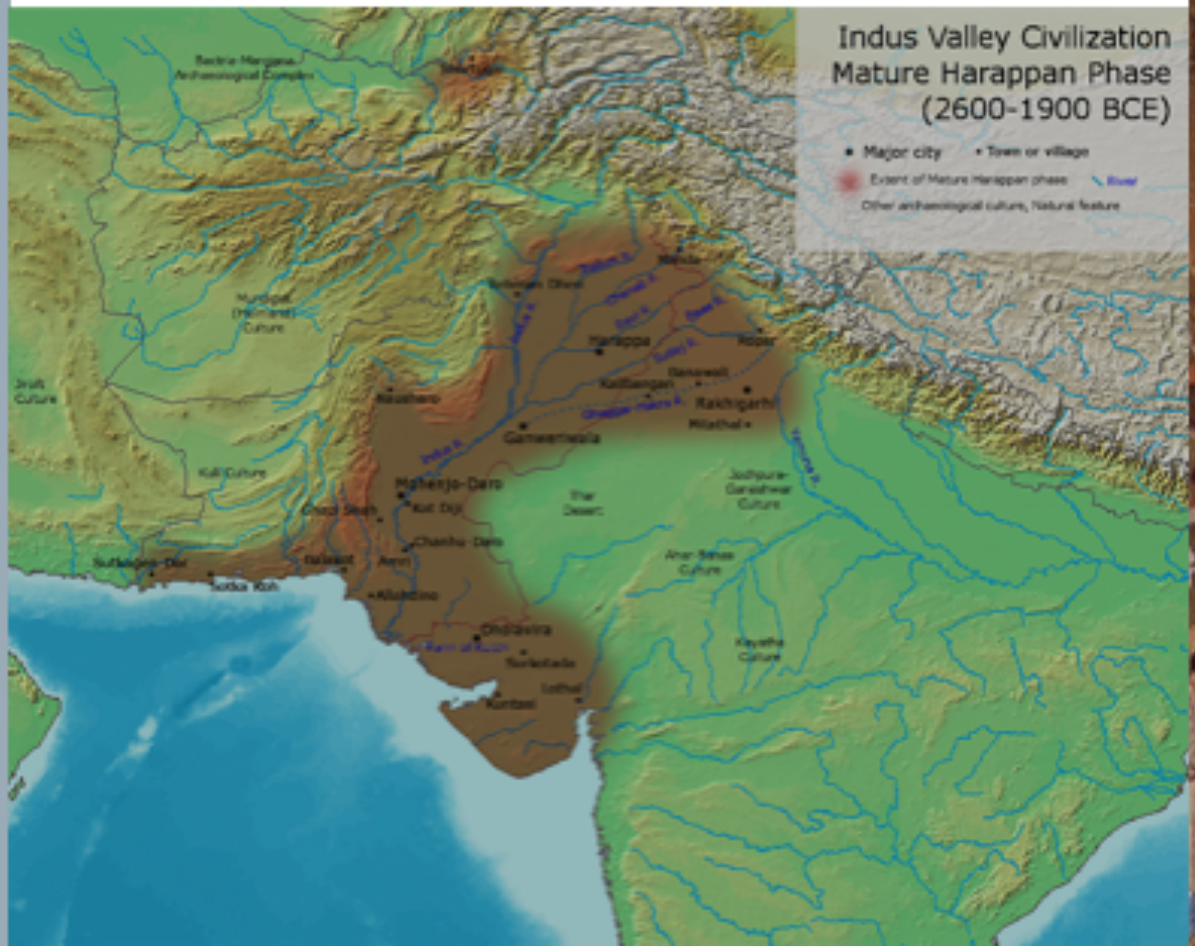
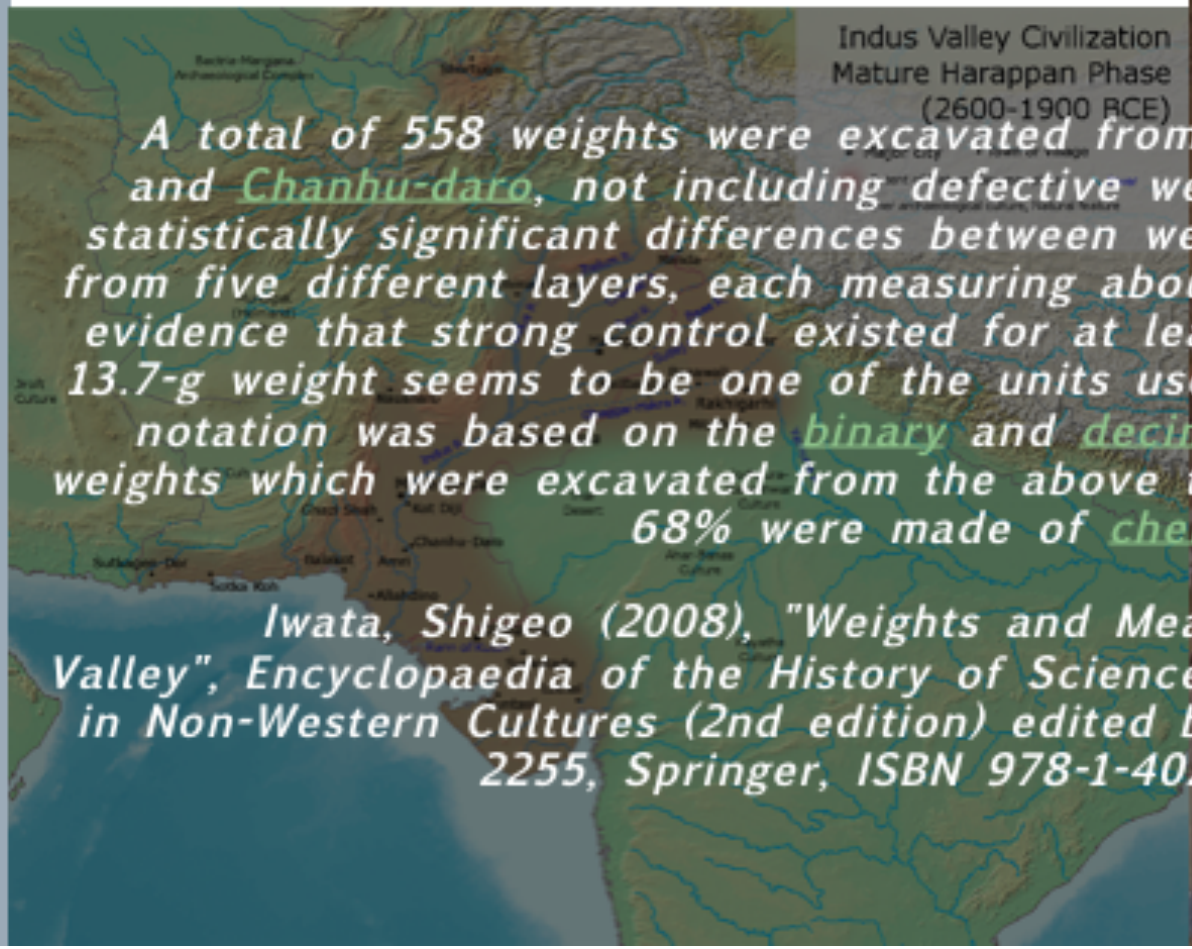
# Padrões e Conformidade

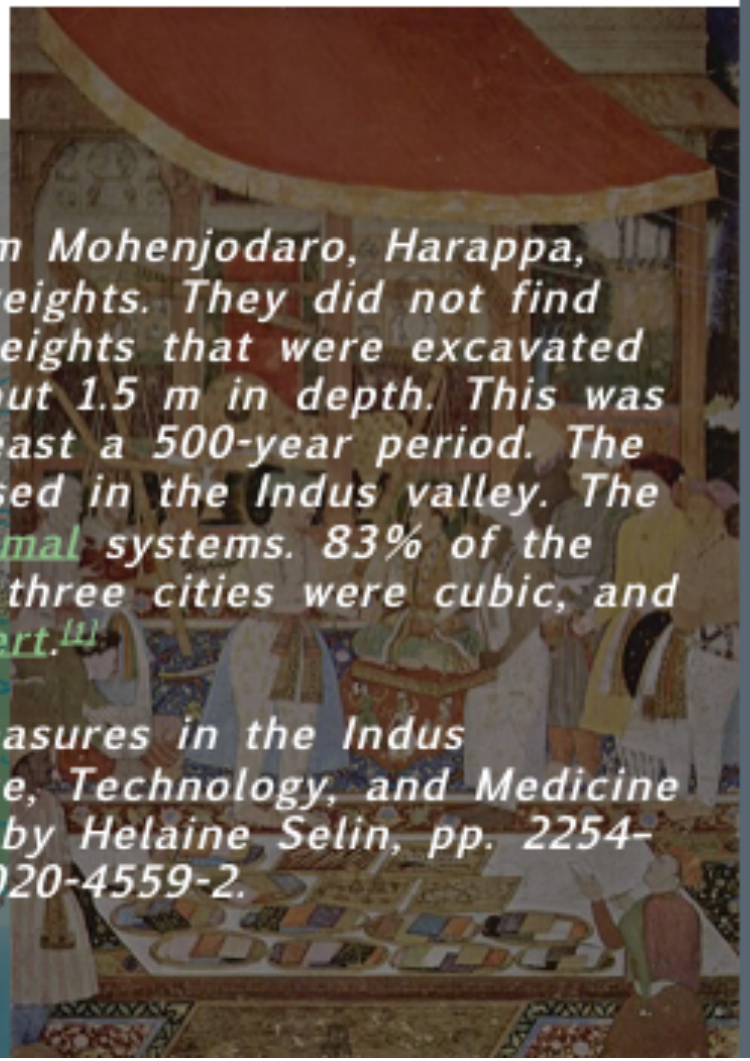
## Padronização e Avaliação da Conformidade na Área de Segurança

# Padrões, pesos e medidas: origens da metrologia científica




# Padrões, pesos e medidas: origens na metrologia científica



*A total of 558 weights were excavated from Mohenjodaro, Harappa, and Chanhu-daro, not including defective weights. They did not find statistically significant differences between weights that were excavated from five different layers, each measuring about 1.5 m in depth. This was evidence that strong control existed for at least a 500-year period. The 13.7-g weight seems to be one of the units used in the Indus valley. The notation was based on the binary and decimal systems. 83% of the weights which were excavated from the above three cities were cubic, and 68% were made of chert.*[1]

*Iwata, Shigeo (2008), "Weights and Measures in the Indus Valley", Encyclopaedia of the History of Science, Technology, and Medicine in Non-Western Cultures (2nd edition) edited by Helaine Selin, pp. 2254–2255, Springer, ISBN 978-1-4020-4559-2.*

# Tópicos Históricos da Padronização

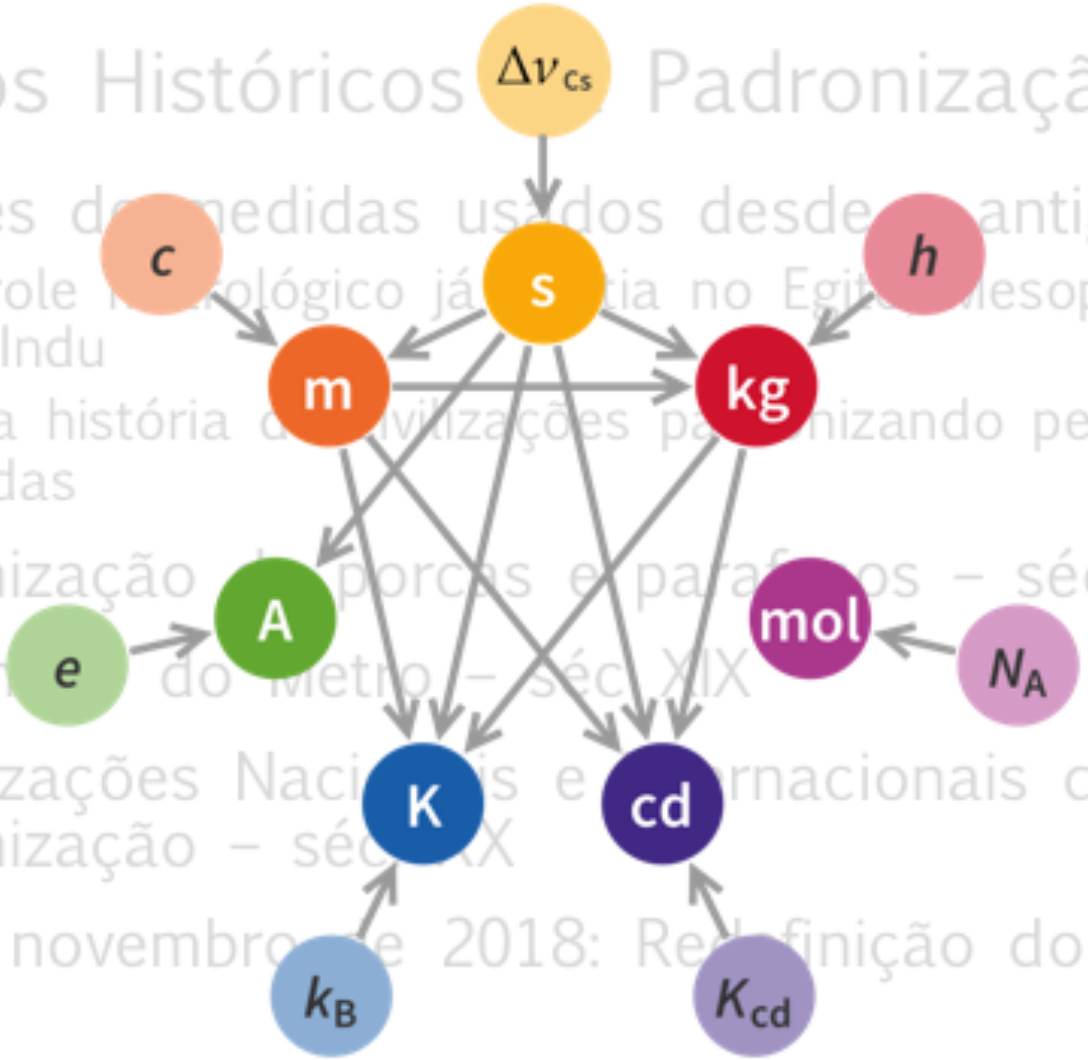
- Padrões de medidas usados desde a antiguidade
  - Controle metrológico já existia no Egito, Mesopotamia e Vale Indu
  - Longa história de civilizações padronizando pesos e medidas
- Padronização de porcas e parafusos – séc. XVIII
- Convenção do Metro – séc XIX
- Organizações Nacionais e Internacionais de Padronização – séc. XX
- 16 de novembro de 2018: Redefinição do SI

# Histórico da Padronização

- Padrões de medidas usados desde a antiguidade
  - Controle metrológico já existia no vale indu
- Padronização de porcas e parafusos – séc. XVIII
- Organizações Nacionais de Padronização – séc. XX
  - 1901: Engineering Standards Committee (Inglaterra)
  - 1917: Deutsches Institut für Normung (Alemanha)
  - 1918: American National Standard Institute (EUA)
  - 1918: Commission Permanente de Standardisation (França)
- Padronização internacional:
  - formação da IEC (International Electrotechnical Commission) em 1906
  - fundação da ISA (depois ISO) em 1926 (resp. 1946)

# Tópicos Históricos da Padronização

- Padrões de medidas usados desde a antiguidade
  - Controle metrológico já existia no Egito, Mesopotamia e Vale Indu
  - Longa história de civilizações padronizando pesos e medidas
- Padronização de toneladas e parafusos – séc. XVIII
- Convenção do Metro – séc. XIX
- Organizações Nacionais e Internacionais de Padronização – séc. XX
- 16 de novembro de 2018: Redefinição do SI



# Ex.: Padronização de Tempo (UTC)

**BUREAU INTERNATIONAL DES POIDS ET MESURES**

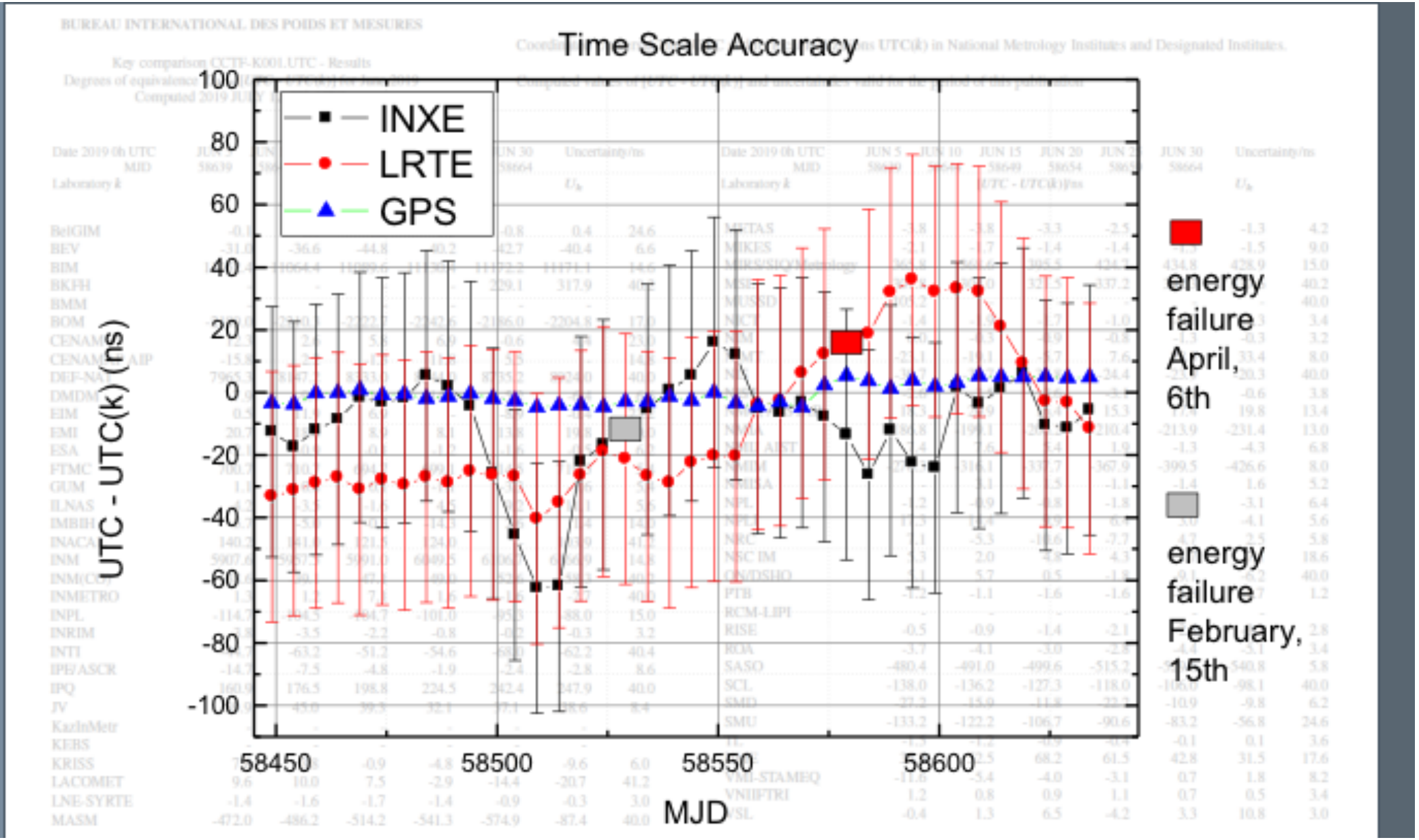
Key comparison CCTF-K001.UTC - Results
Degrees of equivalence $D_k = [UTC - UTC(k)]$ for June 2019
Computed 2019 JULY 12, 09h UTC

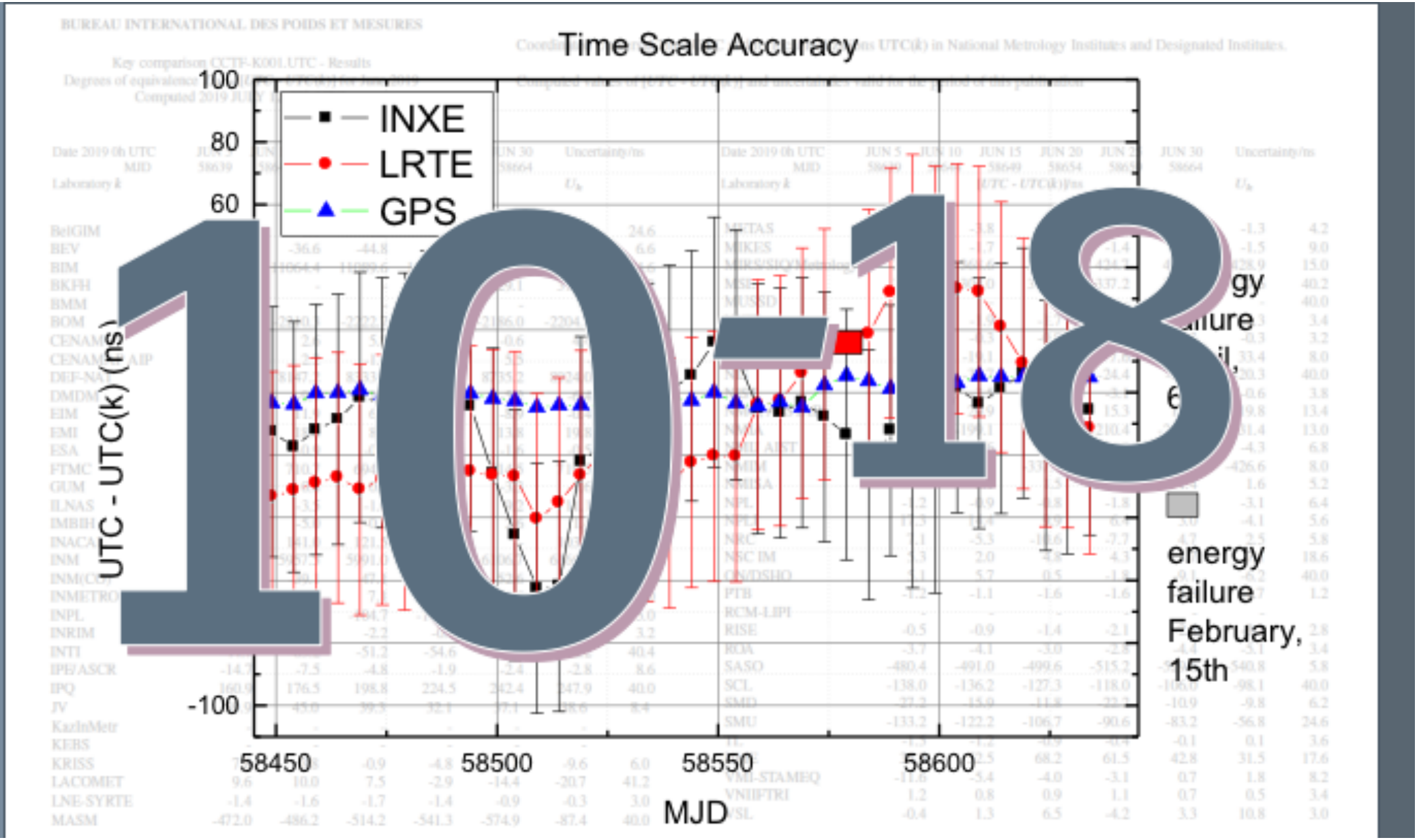
Coordinated Universal Time **UTC** and its local realizations **UTC(k)** in National Metrology Institutes and Designated Institutes.

Computed values of $[UTC - UTC(k)]$ and uncertainties valid for the period of this publication

| Date 2019 0h UTC | JUN 5 | JUN 10 | JUN 15 | JUN 20 | JUN 25 | JUN 30 | Uncertainty/ns |
|---|---|---|---|---|---|---|---|
| MJD | 58639 | 58644 | 58649 | 58654 | 58659 | 58664 | |
| Laboratory *k* | $[UTC - UTC(k)]$/ns | | | | | | $U_k$ |
| BelGIM | -0.1 | -0.8 | -1.3 | -1.5 | -0.8 | 0.4 | 24.6 |
| BEV | -31.0 | -36.6 | -44.8 | -40.2 | -42.7 | -40.4 | 6.6 |
| BIM | 11052.4 | 11064.4 | 11089.6 | 11130.4 | 11172.2 | 11171.1 | 14.6 |
| BKFH | - | - | - | - | 229.1 | 317.9 | 40.2 |
| BMM | - | - | - | - | - | - | |
| BOM | -2189.0 | -2210.3 | -2222.7 | -2242.6 | -2186.0 | -2204.8 | 17.0 |
| CENAM | 12.3 | 2.6 | 5.8 | 6.9 | -0.6 | 4.4 | 23.0 |
| CENAMAP AIP | -15.8 | 2.2 | -1.3 | 11.8 | 5.5 | - | 14.8 |
| DEF-NAT | 7965.3 | 8147.2 | 8333.0 | 8544.0 | 8735.2 | 8924.0 | 40.0 |
| DMDM | -7.9 | -9.7 | -11.2 | -14.5 | -5.2 | -6.4 | 6.6 |
| EIM | 0.5 | 11.9 | 6.9 | - | -8.9 | -0.4 | 23.2 |
| EMI | 20.7 | 18.0 | 8.9 | 8.1 | 13.8 | 19.8 | 19.0 |
| ESA | -2.1 | -0.9 | -0.1 | -1.2 | -1.6 | -0.5 | 6.2 |
| FTMC | 700.7 | 710.7 | 694.7 | 699.1 | 714.5 | 719.5 | 5.4 |
| GUM | 1.1 | 0.8 | 0.1 | -1.1 | -3.3 | -5.6 | 5.4 |
| ILNAS | -4.2 | -3.5 | -1.6 | 4.5 | 9.2 | 11.1 | 5.6 |
| IMBIH | -5.7 | -5.0 | -0.3 | -14.3 | 2.6 | 1.4 | 14.0 |
| INACAL | 140.2 | 141.0 | 121.5 | 124.0 | - | 103.9 | 41.2 |
| INM | 5907.6 | 5957.5 | 5991.0 | 6049.5 | 6106.7 | 6166.9 | 14.8 |
| INM(CO) | -38.6 | -39.1 | -47.1 | -49.0 | -52.6 | -58.3 | 40.2 |
| INMETRO | 1.3 | 1.2 | 7.1 | 1.6 | -1.6 | -2.7 | 40.0 |
| INPL | -114.7 | -104.5 | -104.7 | -101.0 | -95.3 | -88.0 | 15.0 |
| INRIM | -3.8 | -3.5 | -2.2 | -0.8 | -0.2 | -0.3 | 3.2 |
| INTI | -44.7 | -63.2 | -51.2 | -54.6 | -68.0 | -62.2 | 40.4 |
| IPE/ASCR | -14.7 | -7.5 | -4.8 | -1.9 | -2.4 | -2.8 | 8.6 |
| IPQ | 160.9 | 176.5 | 198.8 | 224.5 | 242.4 | 247.9 | 40.0 |
| JV | 39.9 | 45.0 | 39.3 | 32.1 | 37.1 | 38.6 | 8.4 |
| KazInMetr | - | - | - | - | - | - | |
| KEBS | - | - | - | - | - | - | |
| KRISS | 7.8 | 3.8 | -0.9 | -4.8 | -8.1 | -9.6 | 6.0 |
| LACOMET | 9.6 | 10.0 | 7.5 | -2.9 | -14.4 | -20.7 | 41.2 |
| LNE-SYRTE | -1.4 | -1.6 | -1.7 | -1.4 | -0.9 | -0.3 | 3.0 |
| MASM | -472.0 | -486.2 | -514.2 | -541.3 | -574.9 | -87.4 | 40.0 |

| Date 2019 0h UTC | JUN 5 | JUN 10 | JUN 15 | JUN 20 | JUN 25 | JUN 30 | Uncertainty/ns |
|---|---|---|---|---|---|---|---|
| MJD | 58639 | 58644 | 58649 | 58654 | 58659 | 58664 | |
| Laboratory *k* | $[UTC - UTC(k)]$/ns | | | | | | $U_k$ |
| METAS | -3.8 | -3.8 | -3.3 | -2.5 | -1.6 | -1.3 | 4.2 |
| MIKES | -2.1 | -1.7 | -1.4 | -1.4 | -1.5 | -1.5 | 9.0 |
| MIRS/SIQ/Metrology | 365.8 | 368.6 | 395.5 | 424.7 | 434.8 | 428.9 | 15.0 |
| MSL | 307.8 | 304.0 | 321.5 | 337.2 | 342.3 | 337.6 | 40.2 |
| MUSSD | 105.2 | - | - | - | - | - | 40.0 |
| NICT | -1.4 | -1.9 | -1.7 | -1.0 | -0.7 | -1.3 | 3.4 |
| NIM | 0.0 | -0.3 | -0.9 | -0.8 | -1.3 | -0.3 | 3.2 |
| NIMT | -23.1 | -19.1 | -5.7 | 7.6 | 28.3 | 33.4 | 8.0 |
| NIS | -30.7 | -37.7 | -34.8 | -24.4 | -23.9 | -20.3 | 40.0 |
| NIST | -2.6 | -3.5 | -3.6 | -3.1 | -1.9 | -0.6 | 3.8 |
| NMC, A*STAR | 18.3 | 20.9 | 16.4 | 15.3 | 17.4 | 19.8 | 13.4 |
| NMIA | -186.8 | -199.1 | -206.2 | -210.4 | -213.9 | -231.4 | 13.0 |
| NMIJ AIST | 7.4 | 7.6 | 5.4 | 1.9 | -1.3 | -4.3 | 6.8 |
| NMIM | -278.3 | -316.1 | -337.7 | -367.9 | -399.5 | -426.6 | 8.0 |
| NMISA | - | 3.1 | 1.5 | -1.1 | -1.4 | 1.6 | 5.2 |
| NPL | -1.2 | -0.9 | -0.8 | -1.8 | -2.3 | -3.1 | 6.4 |
| NPLI | 17.3 | 14.4 | 9.9 | 6.4 | 3.0 | -4.1 | 5.6 |
| NRC | 7.1 | -5.3 | -10.6 | -7.7 | 4.7 | 2.5 | 5.8 |
| NSC IM | 5.3 | 2.0 | 4.8 | 4.3 | 1.7 | 7.1 | 18.6 |
| ON/DSHO | 5.1 | 5.7 | 0.5 | -1.8 | -9.1 | -6.2 | 40.0 |
| PTB | -1.2 | -1.1 | -1.6 | -1.6 | -1.8 | -1.7 | 1.2 |
| RCM-LIPI | - | - | - | - | - | - | |
| RISE | -0.5 | -0.9 | -1.4 | -2.1 | -2.8 | -3.1 | 2.8 |
| ROA | -3.7 | -4.1 | -3.0 | -2.8 | -4.4 | -5.1 | 3.4 |
| SASO | -480.4 | -491.0 | -499.6 | -515.2 | -529.6 | -540.8 | 5.8 |
| SCL | -138.0 | -136.2 | -127.3 | -118.0 | -106.0 | -98.1 | 40.0 |
| SMD | -27.2 | -15.9 | -11.8 | -22.2 | -10.9 | -9.8 | 6.2 |
| SMU | -133.2 | -122.2 | -106.7 | -90.6 | -83.2 | -56.8 | 24.6 |
| TL | -1.5 | -1.2 | -0.9 | -0.4 | -0.1 | 0.1 | 3.6 |
| UME | 35.5 | 52.5 | 68.2 | 61.5 | 42.8 | 31.5 | 17.6 |
| VMI-STAMEQ | -11.6 | -5.4 | -4.0 | -3.1 | 0.7 | 1.8 | 8.2 |
| VNIIFTRI | 1.2 | 0.8 | 0.9 | 1.1 | 0.7 | 0.5 | 3.4 |
| VSL | -0.4 | 1.3 | 6.5 | -4.2 | 3.3 | 10.8 | 3.0 |


Time Scale Accuracy
INXE
LRTE
GPS
UTC - UTC(k) (ns)
MJD
100
80
60
40
20
0
-20
-40
-60
-80
-100
58450
58500
58550
58600
energy failure April, 6th
energy failure February, 15th

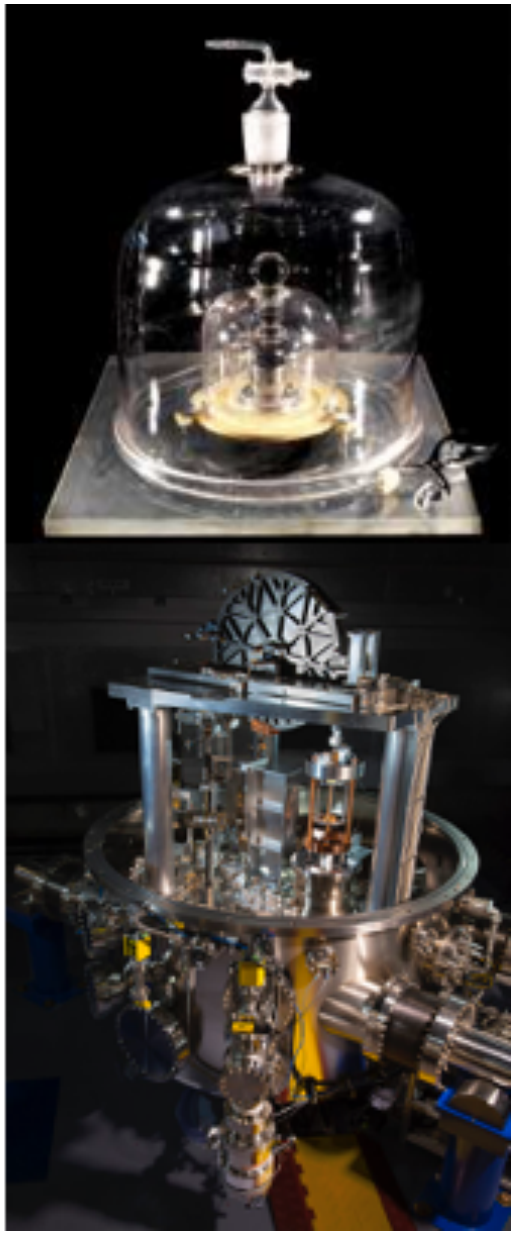

Time Scale Accuracy
INXE
LRTE
GPS
UTC - UTC(k) (ns)
100
80
60
-100
58450
58500
58550
58600
MJD
10-18
energy
failure
February,
15th

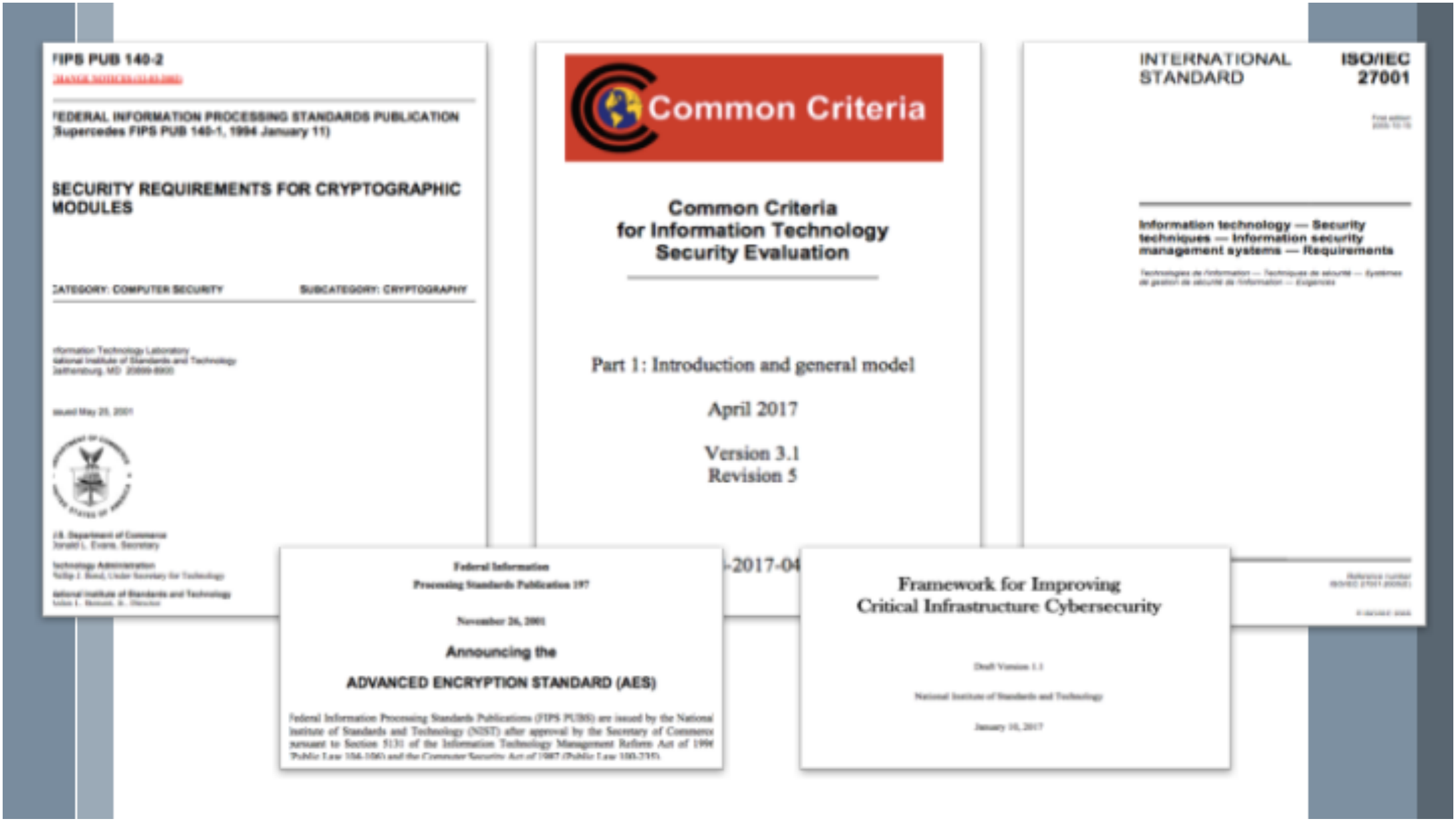
# Importância dos padrões metrológicos

- Comércio
  - Muitos negócios baseiam-se em massa, área, volume – e até grandezas mais "inesperadas" (umidade, poder calorífico,...)
- Tributação
  - Governos também precisam saber das "quantidades" negociadas para aplicar taxação
- Indústria
  - Peças produzidas em diferentes países precisam "se encaixar"
  - Propriedades químicas de insumos para processos industriais
- Ciência
  - "*Metrology is key to reproducing results*" - Nature 547 (jul-2017)

# Que padrões...?

- Padrões de referência de grandezas físicas
  - Metrologia científica "clássica" (SI)
  - Materiais de referência (inclusive biológicos)
  - Peças e ferramentas, processos industriais,...
- Padrões de software e segurança cibernética
  - Definições claras e rigorosas das "referências"
  - Padrão *versus* norma
- Exemplos de padrões de software/segurança
  - Algoritmo criptográficos (ex. AES)
  - Segurança de Hardware (ex. FIPS 140-2)
  - Metodologia de gestão de riscos (ex. NIST CSF)
  - Esquemas de validação de software (ex. CC)
  - Sistema de Gestão (ex. ISO/IEC 27001)
  - Auditoria de Labs (NVLAP Handbooks 150-17)





FIPS PUB 140-2

CHANGE NOTICES (12-03-2002)

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
(Supercedes FIPS PUB 140-1, 1994 January 11)

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

CATEGORY: COMPUTER SECURITY SUBCATEGORY: CRYPTOGRAPHY

nformation Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

issued May 25, 2001

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology
[illegible], Director

Common Criteria

Common Criteria
for Information Technology
Security Evaluation

Part 1: Introduction and general model

April 2017

Version 3.1
Revision 5

-2017-04

INTERNATIONAL STANDARD ISO/IEC 27001

First edition
2005-10-15

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2005(E)

© ISO/IEC 2005

Federal Information
Processing Standards Publication 197

November 26, 2001

Announcing the

ADVANCED ENCRYPTION STANDARD (AES)

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235).

Framework for Improving
Critical Infrastructure Cybersecurity

Draft Version 1.1

National Institute of Standards and Technology

January 10, 2017

# Importância da Padronização

- Padrões representam a convergência técnica entre os maiores especialistas em um assunto
  - Descrevem as melhores práticas em relação àquele assunto
- Definem uma base conceitual e nomenclatura comum
  - Facilitam comunicação, medição, comércio e interoperabilidade
- Promovem boas práticas para a economia:
  - facilitam a interação entre empresas
  - facilitam a conformidade a leis e regulações
  - aceleram a introdução de inovações
  - promovem a interoperabilidade entre produtos, serviços e processos – novos e existentes

# Princípios para desenvolvimento de padrões

- Padrões devem ser uma resposta a uma necessidade do mercado ou da sociedade
  - Para serem efetivos, padrões devem ser criados como uma resposta a uma necessidade de um setor do mercado ou da sociedade.
- Padrões devem ser baseados na opinião de especialistas
  - Bons padrões envolvem uma forte participação e liderança de especialistas, os quais negociam todos os detalhes técnicos dos padrões
- Padrões devem ser desenvolvidos numa base "multi-stakeholder"
  - Comitês técnicos responsáveis pelo desenvolvimento de padrões devem incluir especialistas do Governo, Indústria, Academia, Consumidores, Organizações Não-Governamentais e Sociedade, em geral.
- Padrões devem ser baseados em consenso
  - Comentários de todos os stakeholders devem ser levados em consideração

# Padronização de Telecom

- ITU-T (ITU Telecommunication Standardization Sector)
  - 17-mai-1865: assinatura da Convention Télégraphique Internationale de Paris
    - Padrões elétricos e operacionais de telefones e telégrafos
    - Posteriormente, comunicações por rádio
  - Início do Século XX: CCIF, CCIR CCIT
  - 1956: CCITT (Comité Consultatif International Téléphonique et Télégraphique)
  - 1993: ITU-T
- Histórico: padronização de aspectos físicos e elétricos de equipamentos de telecom

# Padronização em TIC

- Organizações internacionais formais
  - ISO/IEC, ITU-T
- Outros fóruns internacionais
  - IETF
- Organizações regionais relevantes
  - IEEE, ETSI
- Instituições de Governos Nacionais relevantes
  - NIST, BSI, ANSSI, NCSC
- Instituições setoriais relevantes
  - PCI SSC, NERC

# IEEE-SA

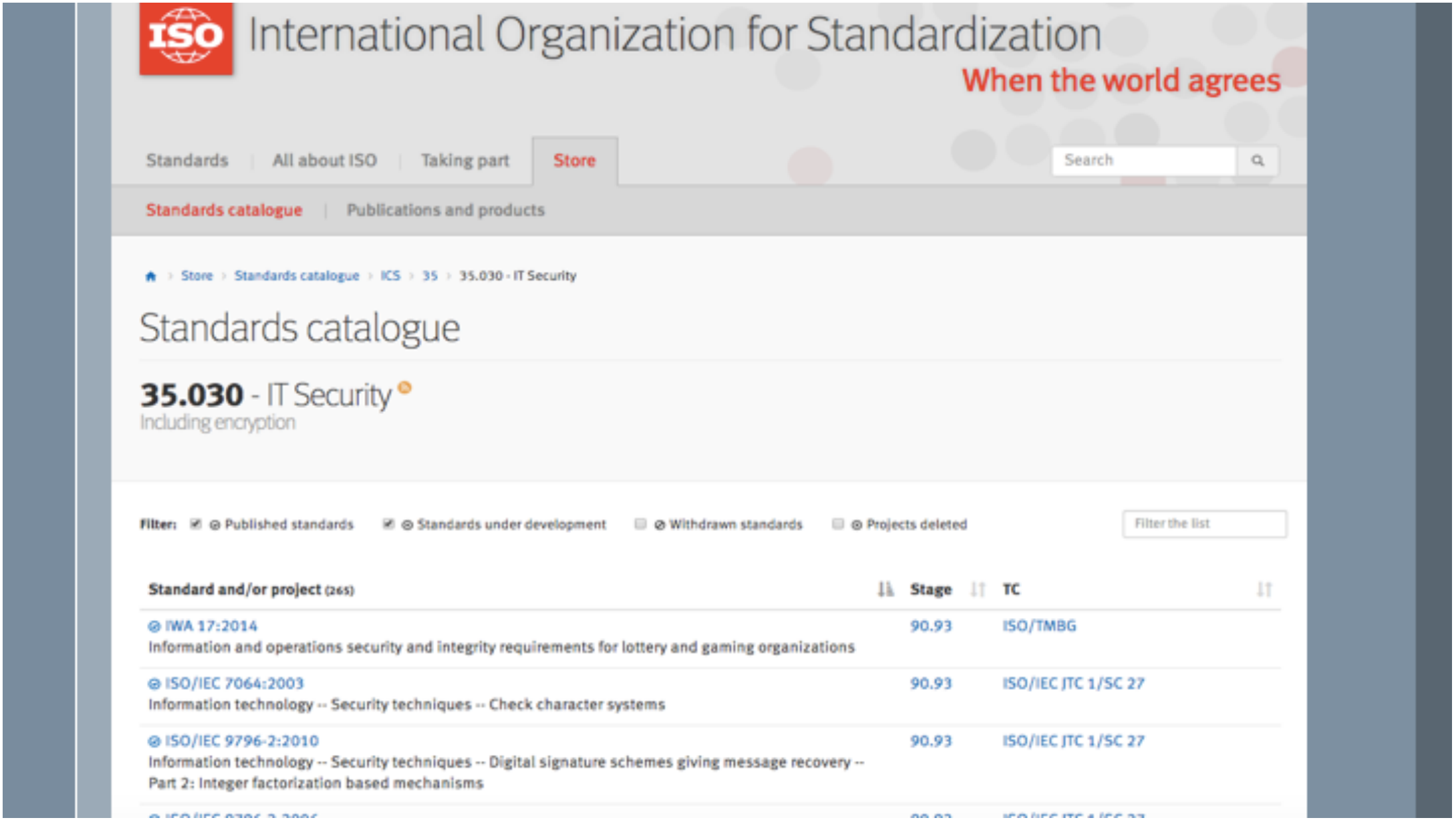
- Institute of Electrical and Electronics Engineers Standards Association
- Padrões em diversas áreas: TI, telecom, energia,...
- Exemplos:
  - 802 Local Area Network (LAN)/Metropolitan Area Network (MAN) Standards Committee
  - tecnologias de rede: wifi (802.11), Bluetooth, Wimax,...

# IETF

- Internet Engineering Task-Force
- Evolução da arquitetura da internet e operação da internet
- Publicação de RFCs (Requests for Comments)
- Exemplos:
  - Domain Name System (DNS) security, authentication protocols, routing protocol security, Internet Protocol (IP) version 6, public key infrastructure, e-mail security, event logging, network traffic encryption

# ISO

- International Organization for Standardization
- Mais de 150 países membros
- Aborda padrões de todas as áreas
- Padrões de elétrica/eletrônica são desenvolvidos em conjunto com IEC (JTC1)
- Exemplos:
  - Grupo SC17: cartões de identificação e identificação pessoal
  - Grupo SC27: técnicas de segurança de TI
  - Grupo SC31: identificação automática e captura de dados
  - Grupo SC37: padrões biométricos


International Organization for Standardization
When the world agrees
Standards
All about ISO
Taking part
Store
Search
Standards catalogue
Publications and products
Store › Standards catalogue › ICS › 35 › 35.030 - IT Security
Standards catalogue
35.030 - IT Security
Including encryption
Filter: Published standards Standards under development Withdrawn standards Projects deleted
Filter the list
Standard and/or project (265)
Stage
TC
IWA 17:2014
Information and operations security and integrity requirements for lottery and gaming organizations
90.93
ISO/TMBG
ISO/IEC 7064:2003
Information technology -- Security techniques -- Check character systems
90.93
ISO/IEC JTC 1/SC 27
ISO/IEC 9796-2:2010
Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms
90.93
ISO/IEC JTC 1/SC 27

# ITU-T

- ITU Telecommunication Standardization Sector
- Produz padrões chamados *Recommendations*, para redes de comunicação
- O grupo de estudo 17 (SG17) coordena os trabalhos relacionados a segurança entre todos os grupos de estudo do ITU-T.
- Exemplos:
  - X.800: Security architecture for Open Systems Interconnection for CCITT applications
  - Recommendation ITU-T X.509 for electronic authentication over public networks

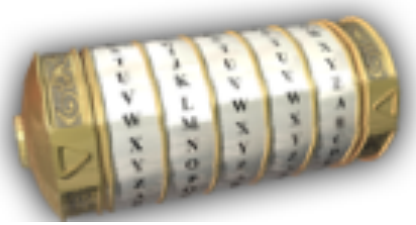
# Padronização e Avaliação da Conformidade

- Padrões frequentemente têm foco nos "requisitos"
  - Mas é importante saber avaliar se os padrões estão sendo alcançados
- Testes de conformidade permitem avaliar o atendimento aos requisitos de um padrão
  - Realizados através de ensaios, inspeções, auditorias etc.
- Avaliação da Conformidade têm seus próprios padrões (ISO série 17000)

# Padronização versus Obscurantismo

# Obscurantismo

- Princípio através do qual se protege a Segurança de um sistema por meio do Segredo/Sigilo dos seus detalhes de implementação
- Conceito predominante até o século XIX por meio da esteganografia
- O tratamento cada vez mais "científico" da Segurança Cibernética - apoiado por disciplinas como Criptografia, Complexidade Computacional, Especificação Formal,... - tem relegado o obscurantismo a uma posição bastante restrita.
- O conceito ainda é bastante difundido em setores como Governo, Diplomacia, Militar/Defesa...



# Padronização versus obscurantismo

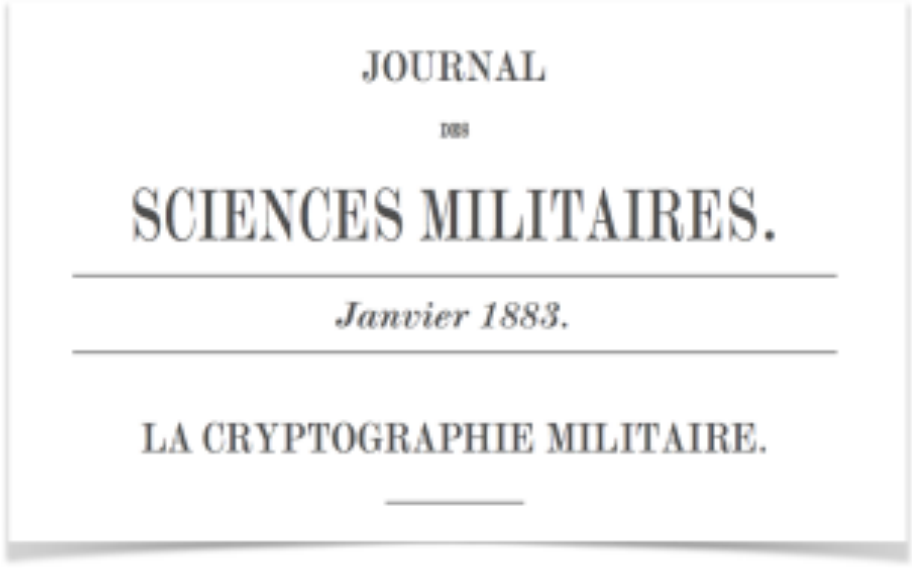
- Padronização versus obscurantismo: uma decisão técnica e política
  - Obscurantismo tem seu lugar em aplicações específicas
  - Mas para a maioria das aplicações, não é prático ou realístico
- Desvantagens do obscurantismo
  - Não pode ser garantida ao longo do tempo
    - Equipamentos criptográficos podem ser capturados por inimigo
    - Desenvolvedores de software mudam de empresa (para o concorrente!)
  - Reduz a visibilidade pelos usuários a respeito das funcionalidades do sistema
    - Como se ter certeza de que um equipamento sensível não está sujeito a manipulações?

# Desvantagens do Obscurantismo

- Não pode ser garantida ao longo do tempo
  - Equipamentos criptográficos podem ser capturados por inimigo
  - Desenvolvedores de software mudam de empresa (para o concorrente!)
- Reduz a visibilidade pelos usuários a respeito das funcionalidades do sistema
  - Como o cidadão pode ter certeza de que um equipamento sensível (por exemplo, uma urna eletrônica ou um medidor inteligente) não está sujeito a manipulações?

# Princípios de Criptografia de Kerckhoff

## › DESIDERATA DE LA CRYPTOGRAPHIE MILITAIRE



JOURNAL

DES

SCIENCES MILITAIRES.

*Janvier 1883.*

LA CRYPTOGRAPHIE MILITAIRE.

1° Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;

2° Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;

3° La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;

4° Il faut qu'il soit applicable à la correspondance télégraphique ;

5° Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;

6° Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

# Por que padrões...

- Permitem ”refletir” para soluções locais as referências e boas práticas internacionais
- Padrões forçam o exercício do método científico
  - Descrição rigorosa de conceitos, requisitos e métodos
  - Compreensão plena e domínio técnico
- Padrões facilitam a propagação de informação
  - Estimulam a implantação de soluções de segurança
  - Caso do DES (Data Encryption Standard) – prox. slide

# Requisitos do Data Encryption Standard

- The algorithm must provide a high level of security.
- The algorithm must be completely specified and easy to understand.
- The security of the algorithm must reside in the key; the security should not depend on the secrecy of the algorithm.
- The algorithm must be available to all users.
- The algorithm must be adaptable for use in diverse applications.
- The algorithm must be economically implementable in electronic devices.
- The algorithm must be efficient to use.
- The algorithm must be able to be validated.
- The algorithm must be exportable.

# Impacto do Data Encryption Standard

- *These standards were unprecedented. Never before had an NSA-evaluated algorithm been made public. [...] DES did more to galvanize the field of cryptanalysis than anything else. Now there was an algorithm to study: one that the NSA said was secure.*

Bruce Schneier, Applied Cryptography

# Padronização, Avaliação da Conformidade e Auditibilidade

- Possibilidade de analisar todas as características e os detalhes de implementação de um sistema
- A estrutura de Padronização Técnica e Avaliação da Conformidade leva o conceito de auditibilidade a um novo patamar
  - Modelos avaliação de riscos e especificação de requisitos são padronizadas
  - Metodologias de avaliação da conformidade - ensaios e testes de segurança - são claramente especificados
  - Até mesmo os procedimentos de auditoria são claramente descritos

# Padronização de um Algoritmo Cripto. (AES)

## Exemplo saudável de transição
## Academia -> Governo -> Indústria

# Chamada por algoritmos

Federal Register / Vol. 62, No. 177 / Friday, September 12, 1997 / Notices 48051

**DEPARTMENT OF COMMERCE**

**National Institute of Standards and Technology**

**[Docket No. 970725180–7180–01]**

**RIN No. 0693–ZA16**

**Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard**

**AGENCY:** National Institute of Standards and Technology (NIST), Commerce.

**ACTION:** Notice; Request for candidate encryption algorithm nomination packages.

**SUMMARY:** A process to develop a Federal Information Processing Standard (FIPS) for Advanced Encryption Standard (AES) specifying an Advanced Encryption Algorithm (AEA) has been initiated by the National Institute of Standards and Technology (NIST). This notice requests submission of candidate algorithms for *consideration for inclusion in the* AES and specifies how to submit a nomination package. The requirements for candidate algorithm submission packages and minimum acceptability requirements that must be satisfied in order to be deemed a ''complete and proper'' submission are presented. the evaluation criteria which will be used to appraise the candidate algorithms are also described.

# Cinco Finalistas

Volume 104, Number 5, September–October 1999
Journal of Research of the National Institute of Standards and Technology

[J. Res. Natl. Inst. Stand. Technol. **104**, 435 (1999)]

## *Status Report on the First Round of the Development of the Advanced Encryption Standard*

Volume 104 Number 5 September–October 1999

**James Nechvatal, Elaine Barker, Donna Dodson, Morris Dworkin, James Foti, and Edward Roback**

National Institute of Standards and Technology,
Gaithersburg, MD 20899-0001

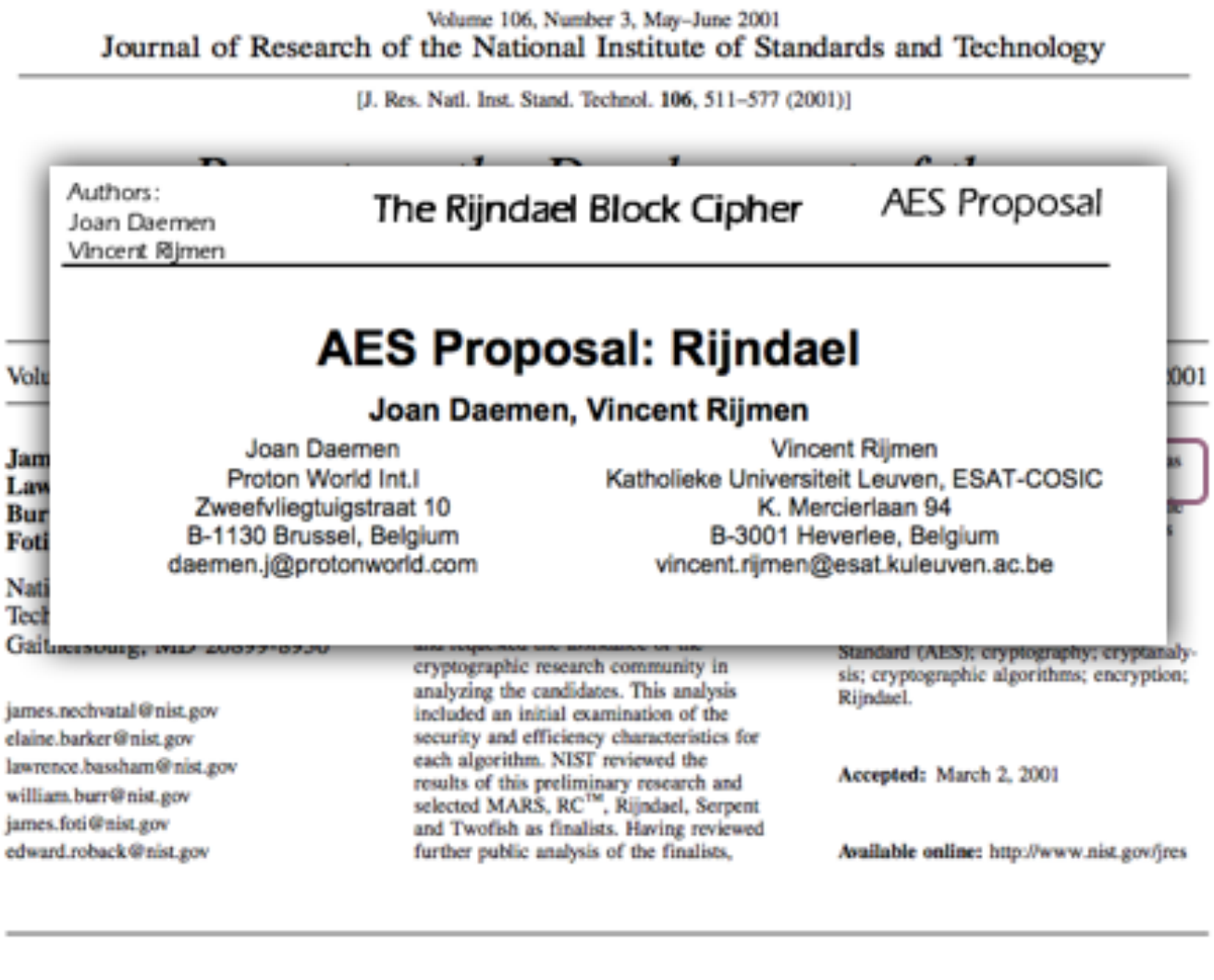
In 1997, the National Institute of Standards and Technology (NIST) initiated a process to select a symmetric-key encryption algorithm to be used to protect sensitive (unclassified) Federal information in furtherance of NIST's statutory responsibilities. In 1998, NIST announced the acceptance of 15 candidate algorithms and requested the assistance of the cryptographic research community in analyzing the candidates. This analysis included an initial examination of the security and efficiency characteristics for each algorithm. NIST has reviewed the results of this research and selected five algorithms (MARS, RC6™, Rijndael, Serpent and Twofish) as finalists. The research results and rationale for the selection of the finalists are documented in this report. The five finalists will be the subject of further study before the selection of one or more of these algorithms for inclusion in the Advanced Encryption Standard.

**Key words:** Advanced Encryption Standard (AES); cryptography; cryptanalysis; cryptographic algorithms; encryption.

**Accepted:** August 11, 1999

**Available online:** http://www.nist.gov/jres

# O escolhido: Rijndael



Volume 106, Number 3, May–June 2001
Journal of Research of the National Institute of Standards and Technology

[J. Res. Natl. Inst. Stand. Technol. **106**, 511–577 (2001)]

Authors:
Joan Daemen
Vincent Rijmen

The Rijndael Block Cipher — AES Proposal

**AES Proposal: Rijndael**

**Joan Daemen, Vincent Rijmen**

Joan Daemen
Proton World Int.l
Zweefvliegtuigstraat 10
B-1130 Brussel, Belgium
daemen.j@protonworld.com

Vincent Rijmen
Katholieke Universiteit Leuven, ESAT-COSIC
K. Mercierlaan 94
B-3001 Heverlee, Belgium
vincent.rijmen@esat.kuleuven.ac.be

james.nechvatal@nist.gov
elaine.barker@nist.gov
lawrence.bassham@nist.gov
william.burr@nist.gov
james.foti@nist.gov
edward.roback@nist.gov

cryptographic research community in analyzing the candidates. This analysis included an initial examination of the security and efficiency characteristics for each algorithm. NIST reviewed the results of this preliminary research and selected MARS, RC™, Rijndael, Serpent and Twofish as finalists. Having reviewed further public analysis of the finalists,

Standard (AES); cryptography; cryptanalysis; cryptographic algorithms; encryption; Rijndael.

**Accepted:** March 2, 2001

**Available online:** http://www.nist.gov/jres

**Federal Information**

**Processing Standards Publication 197**

**November 26, 2001**

## Announcing the

## ADVANCED ENCRYPTION STANDARD (AES)

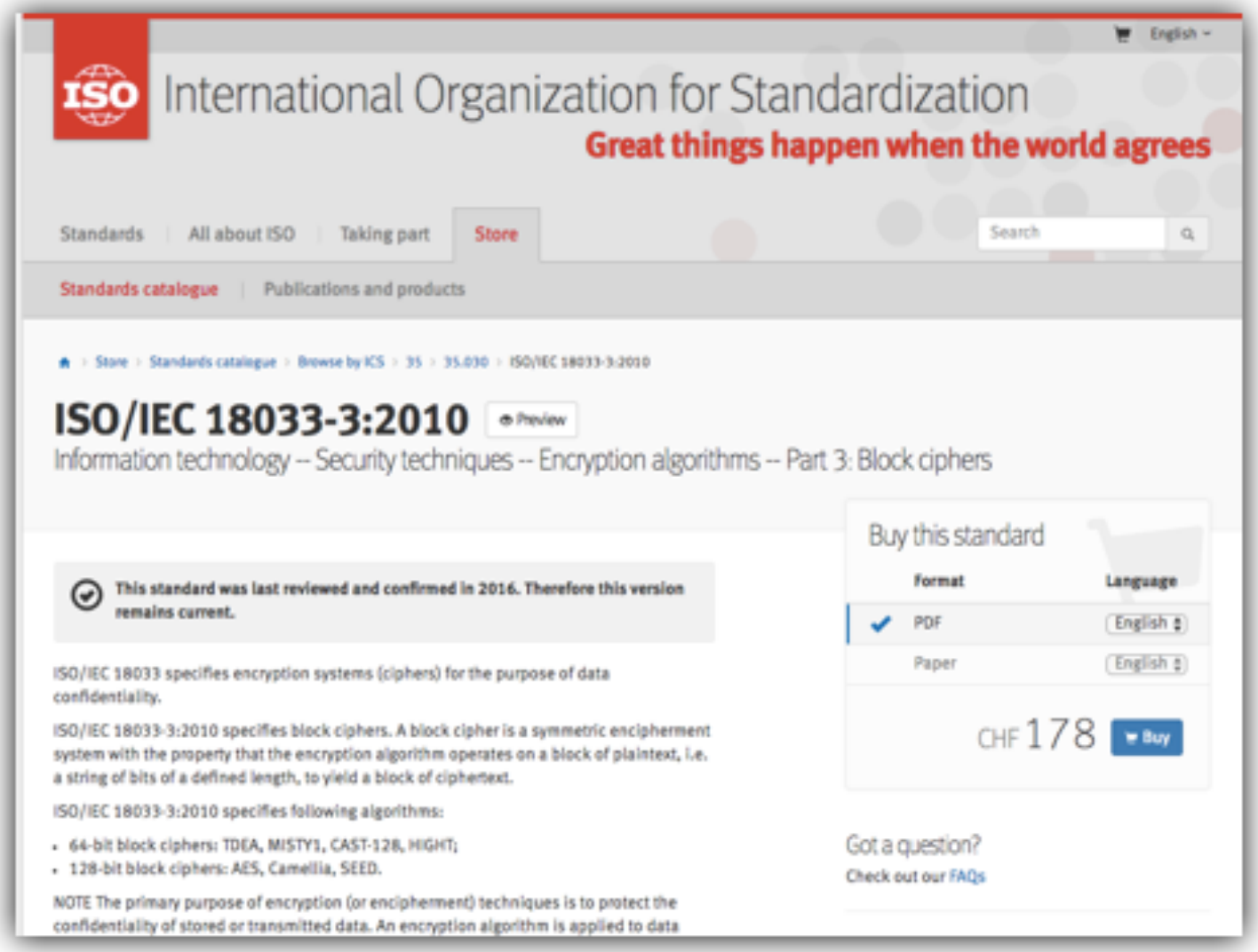
Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235).

1. **Name of Standard.** Advanced Encryption Standard (AES) (FIPS PUB 197).

6. **Applicability.** This standard may be used by Federal departments and agencies when an agency determines that sensitive (unclassified) information (as defined in P. L. 100-235) requires cryptographic protection.

Other FIPS-approved cryptographic algorithms may be used in addition to, or in lieu of, this standard. Federal agencies or departments that use cryptographic devices for protecting classified information can use those devices for protecting sensitive (unclassified) information in lieu of this standard.

In addition, this standard may be adopted and used by non-Federal Government organizations. Such use is encouraged when it provides the desired security for commercial and private organizations.


English
International Organization for Standardization
Great things happen when the world agrees
Standards
All about ISO
Taking part
Store
Search
Standards catalogue
Publications and products
Store › Standards catalogue › Browse by ICS › 35 › 35.030 › ISO/IEC 18033-3:2010
ISO/IEC 18033-3:2010
Preview
Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers
This standard was last reviewed and confirmed in 2016. Therefore this version remains current.
ISO/IEC 18033 specifies encryption systems (ciphers) for the purpose of data confidentiality.
ISO/IEC 18033-3:2010 specifies block ciphers. A block cipher is a symmetric encipherment system with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext.
ISO/IEC 18033-3:2010 specifies following algorithms:
64-bit block ciphers: TDEA, MISTY1, CAST-128, HIGHT;
128-bit block ciphers: AES, Camellia, SEED.
NOTE The primary purpose of encryption (or encipherment) techniques is to protect the confidentiality of stored or transmitted data. An encryption algorithm is applied to data
Buy this standard
Format
Language
PDF
English
Paper
English
CHF 178
Buy
Got a question?
Check out our FAQs

# Avaliação da Conformidade

A medida realizada é válida?
O produto atende ao padrão??

# Regulação, padrões e avaliação da conformidade

- Padrões ferramentas para regulação em todo o mundo
  - Tais padrões podem ser internacionais, nacionais, ou mesmo locais
  - Em alguns casos, apenas partes dos padrões são mandatórios
- Métodos de avaliação da conformidade para atestar o atendimento a requisitos descritos em padrões
  - Regulações podem incluir requisitos para a avaliação da conformidade

# Importância da conformidade

- Padrões só são úteis se forem aderidos/seguidos
- Como fomentar o atendimento ao padrão
  - regulação
- Como demonstrar o atendimento ao padrão
  - avaliação da conformidade

# Avaliação da conformidade

- Definição: conjunto de técnicas e atividades que têm por objetivo garantir que um produto, processo, serviço, sistema de gestão, pessoa ou organização atende a um conjunto de requisitos.
  - Exemplos dessas técnicas e atividades incluem estimação, auditoria, calibração, avaliação, exame, inspeção, e teste
  - Podem resultar numa declaração de conformidade pelo fornecedor, numa certificação ou numa acreditação

# Padrões de Avaliação da Conformidade

- A ISO (International Organization for Standardization) e a IEC (International Electrotechnical Commission) possuem publicações internacionais sobre avaliação da conformidade
  - Essas publicações internacionais são amplamente reconhecidas e usadas nos mais diversos setores e atores para atividades de avaliação da conformidades

# Regulação, padrões e avaliação da conformidade

› Avaliação da conformidade baseada em padrões internacionais
  – favorece o reconhecimento do processo como bem-fundamentado e legítimo.
  – evita que regulações adicionem custos desnecessários e questionamentos quanto a barreiras técnicas ao comércio

# Técnicas de avaliação da conformidade

- **Avaliação (assessment)** da competência técnica de uma organização;
- **Auditoria** de um sistema de gestão de uma organização;
- **Avaliação (evaluation)** de um produto, processo ou serviço em relação a um conjunto de requisitos;
- **Exame** da competência de uma pessoa;
- **Inspeção** de uma instalação, produto ou serviço;
- **Teste** de uma característica de produto.

# Padrões de AC mais relevantes

- ISO/IEC DIS 17000 [Under development]
  - Conformity assessment -- Vocabulary and general principles
- ISO/IEC 17011:2017
  - Conformity assessment -- Requirements for accreditation bodies accrediting conformity assessment bodies
- ISO/IEC 17020:2012
  - Conformity assessment -- Requirements for the operation of various types of bodies performing inspection
- ISO/IEC 17021 (várias partes)
  - Conformity assessment -- Requirements for bodies providing audit and certification of management systems
- ISO/IEC 17025:2017
  - General requirements for the competence of testing and calibration laboratories

# Padrões mais relevantes

- ISO 17034:2016
  - General requirements for the competence of reference material producers
- ISO/IEC 17040:2005
  - Conformity assessment -- General requirements for peer assessment of conformity assessment bodies and accreditation bodies
- ISO/IEC 17043:2010
  - Conformity assessment -- General requirements for proficiency testing
- ISO/IEC 17065:2012
  - Conformity assessment -- Requirements for bodies certifying products, processes and services
- ISO/IEC 17067:2013
  - Conformity assessment -- Fundamentals of product certification and guidelines for product certification schemes

# Declarações de Conformidade

- Declarações a respeito do "objeto" de uma avaliação (produto, processo, serviço, sistema de gestão ou organismo)
  - feitas após aplicação de uma ou mais técnicas de avaliação
- Declarações de conformidade podem ser feitas por:
  - **Primeira parte** – pessoa ou organização que fornece o objeto e que é responsável pelo atendimento aos requisitos (exemplo, fabricante);
  - **Segunda parte** – pessoa ou organização que tem interesse no objeto (exemplo, uma cadeia de varejo comprando para revender);
  - **Terceira parte** – pessoa ou organização que é independente de quem fornece ou consome ou objeto (exemplos: laboratório de testes e organismo de certificação imparciais).

# Exemplo de certificação: equip. ICP-Brasil

Cartão utilizado para assinar documento e leitora usada para ler o cartão...

Atendem a requisitos definidos por padrões internacionais

Bureau International des Poids et Mesures

ISO

INTERNATIONAL ACCREDITATION FORUM IAF

INMETRO

Equipamentos

Processos/qualidade

Pessoas

Avaliados por laboratórios acreditados