Title

First Author
Office of XXXX, First Operating Unit

Second Author
Office of XXXX, Second Operating Unit

Third Author
Office of XXXX, Third Operating Unit
Washington, DC

Fourth Author
Fourth Services, Inc.
Reston, Virginia

Fifth Author
Fifth Services, Inc.
Reston, Virginia

Sixth Author
Sixth Services, Inc.
Reston, Virginia

June 01, 2018

National Institute of
Standards and Technology
U.S. Department of Commerce

Abstract

Include a brief abstract of the document. This can be the same text that is used in the NIST-114 form in NIKE. Any acronyms should be spelled out on first use (e.g., "Personal Identity Verification (PIV)…"). Avoid including references in this abstract. Guidance for writing Abstracts:

- Rule of thumb: limit to 200 words or less;
- Address the following questions:
  - What **problem** was examined or what procedure was carried out?
  - What was the **objective** of the activity being documented?
  - What was the **scope** of the activity?
  - What were the **principal conclusions and recommendations**?
- Use complete sentences;
- Acronyms: spell out upon first occurrence;
- Avoid unnecessary contractions or abbreviations;
- Avoid using equations and tables; and
- Avoid using "this draft" in the Abstract, for it can be easily overlooked when the final version is published

Keywords

The following are keywords to be used by search engines and document catalogues.

conditioning functions; entropy source; health testing; min-entropy; noise source; predictors; random number generators

Supplemental Context

An optional section with links to supplemental content that is integral to the document (e.g., Data DOI, URL for GitHub site with supporting documentation/software; project page on CSRC.nist.gov or another NISTsite, etc.). Should not include links to other SPs, FIPS, NISTIRs, etc.—that info should be in a Reference section or footnotes.

Audience

This document is intended for…

Document Conventions

Definitions of terminology for expressing recommended options (i.e., guidance), mandatory requirements, permissible actions, or possibilities. These could alternatively be specified in the introduction (e.g., Section 1), prior to specifying the technical content.

For Draft and Final publications: Per Annex A of the ITL Patent Policy, the document must also define the terminology used to express recommended options (i.e., guidance) and mandatory requirements. Terminology for expressing permissible actions or possibilities should also be defined. These definitions should ideally precede the technical content—possibly in a Document Conventions section in the front matter (see previous page) or in a subsection of the Introduction (e.g., in Section 1).

Example language is included in Annex A of ITL's Patent Policy (https://www.nist.gov/itl/publications-0/itl-patent-policy-inclusion-patents-itl-publications#annexa) and in the FAQ (https://inet.nist.gov/itl/frequently-asked-questions-itl-patent-policy-inclusion-patents-itl-publications).

For FINAL publication only. If the present document revises/supersedes another publication, consider adding a very brief list that highlights changes/updates in the current version.

Trademark Information

…

Acknowledgements

For guidance on acknowledgements, see NIST Directive G 5201.01, *Guidance for Authorship of Scholarly and Technical Publications*, https://inet.nist.gov/directives/guidance-authorship-scholarly-technical-publications: "Personal Acknowledgement: Formal acknowledgement in a technical publication shall be accorded to individuals who have made at least one contribution to the project. Such contributions can be of any type not meeting the requirements for authorship. Examples include routine programming support, laboratory equipment set-up, useful discussions, or extensive copy-editing of the publication."

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST, nor does it imply that the products mentioned are necessarily the best available for the purpose.

Additional Information

For additional information on NIST's Cybersecurity programs, projects and publications, visit the Computer Security Resource Center. Information on other efforts at NIST and in the Information Technology Laboratory (ITL) is also available.

Feedback

Feedback on this publication is welcome, and can be sent to: code-signing@nist.gov.

1. Introduction

Text

\[Wherever a link is included, e.g., https://www.nist.gov or [FIPS 140-2], add a ScreenTip to the link for Section 508 (accessibility) compliance. Right-click the link and select "ScreenTip" in the pop-up window. Add a generic statement, e.g., "Article link", "NIST report link", "Web page link", etc.]

1.1. Second-level Heading

1.1.1. Third-level Heading

1.1.1.1. Fourth-level Heading

1.2. Subsection Two

Table info

Table 1 — Caption for Table One

Column Header 1	Column Header 2
A	B
C	D

> Admonitions (like [TIP]) are used for text in boxes.

1.3. Document ConventionsA

If this is included in Section 1, it can be included as any subsection number. This just happens to be 1.3 in this template.

This section is unlikely to be needed in a white paper, but if the document includes any permissible actions or possibilities (e.g., "may", "may not", "can", cannot"), then that terminology should be defined. This should ideally precede the technical content, possibly in an introductory subsection like this, or in the front matter (see "Document Conventions", above).

1.4. Subsection Four

General Guidance for References and Footnotes:

TEXT TO BE FINALISED ONCE NUMERIC REFERENCES IMPLEMENTED

References: Authors can choose between using numeric ("[1]") and alphanumeric ("[SP 800-300]") references but should use one or the other.

Authors should only use AsciiDoc cross-references in the body of the text; Metanorma will automatically insert the appropriate numeric or alphanumeric codes, retrieved from the References entry with the same cross-reference.

Numeric references will start with [1] and proceed sequentially for each new reference. If beginning a sentence with a numeric reference, start the sentence with "Reference [xyz]" (which will be rendered as "Reference [n]").

Alphanumeric references can be useful when there are numerous references to other specifications, and having the document number as part of the reference provides useful context to the reader (so they don't have to constantly navigate to the references section to see what's being cited).

Instead of hyperlinking a reference to an external URL, references should be either linked or cross-referenced to the applicable reference in the References section/appendix. Include the correct URL or DOI in the reference. If it ever needs to be update, it can then be (easily!) updated in just one place in the document.

Footnotes[1] can be used but should be used to provide context to the footnoted text. If the footnote includes a link to a referenced source, provide a link or cross-reference to the reference in the References section/appendix

[1] Standard footnote.

2. Section Two Heading

Text.

Figure info:

Improve accessibility by adding Alt Text or each figure.

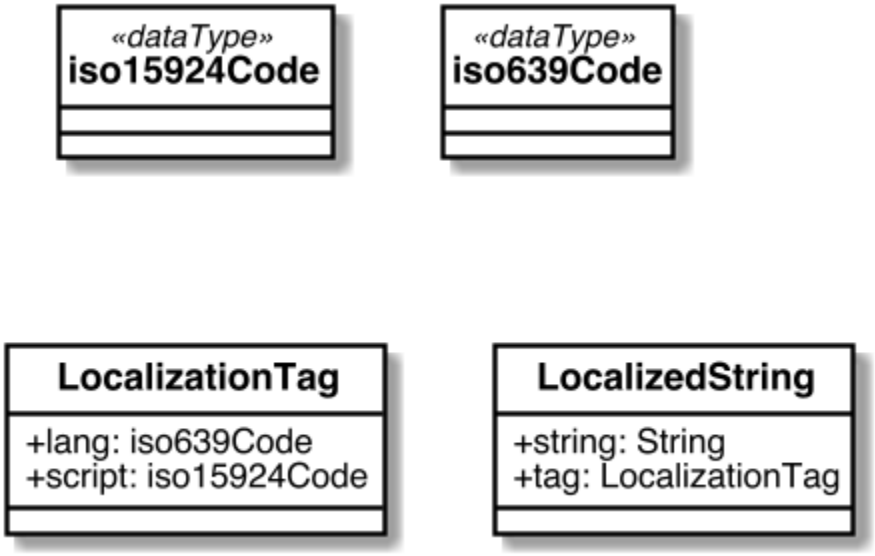

Figure 1 — Caption for Figure One.

Appendix A — Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

Acronym 1	Term 1
Acronym 2	Term 2

Appendix B — Glossary

For the purposes of this document, the following terms and definitions apply.

Term 1
Definition
Term 2
Definitin
Term 3
Definition

Bibliography

[1] Kuhn R, Raunak M, Kacker RN (2017) It Doesn't Have to Be Like This: Cybersecurity Vulnerability Trends. *IT Professional* 19(6):66-70. https://doi.org/10.1109/MITP.2017.4241462

[2] Office of Management and Budget (OMB), *E-Authentication Guidance for Federal Agencies*, OMB Memorandum 04-04, December 16, 2003. Available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2004/m04-04.pdf

[3] Title 32 Code of Federal Regulations, Sec. 2002.4, *Definitions*. July 1, 2018 ed. https://www.govinfo.gov/app/details/CFR-2018-title32-vol6/CFR-2018-title32-vol6-sec2002-4

[4] Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073. https://www.govinfo.gov/app/details/PLAW-113publ283

[5] E-Government Act of 2002, Pub. L. 107-347, 116 Stat 2899. https://www.govinfo.gov/app/details/PLAW-107publ347

[6] Alhebaishi N, Wang L, Jajodia S, Singhal A (2018) Modeling and Mitigating the Insider Threat of Remote Administrators in Clouds. *IFIP Annual Conference on Data and Applications Security and Privacy*, (Springer, 07/10/2018), pp 3-20. https://doi.org/10.1007/978-3-319-95729-6_1

[7] Bhaumik R, Datta N, Dutta A, Mouha N, Nandi M (2017) The Iterated Random Function Problem. *23rd Annual International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2017*, (Springer, 12/07/2017), pp 667-697. https://doi.org/10.1007/978-3-319-70697-9_23

[8] Perlner RA , Liu Y-K (2018) Thermodynamic Analysis of Classical and Quantum Search Algorithms. *Quantum Information Processing*, (Delft, The Netherlands). https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=924493

[9] Souppaya MP, Regenscheid AR, Cooper DA, Cooley D, Bean C, Jenkins M, Boyle M (2018) *Security Considerations for Code Signing*. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.01262018

[10] U.S. Department of Homeland Security, U.S. Department of Commerce (2018) *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*. (U.S. Department of Commerce, Washington, DC). Available at

https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf

[11] National Institute of Standards and Technology, *Cybersecurity Framework* [Web site]. Available at https://www.nist.gov/cyberframework/

[12] Executive Order no. 13636, *Improving Critical Infrastructure Cybersecurity*, DCPD-201300091, February 12, 2013. https://www.govinfo.gov/app/details/FR-2013-02-19/2013-03915

[13] "Establishment of NIST Smart Grid Advisory Committee and Solicitation of Nominations for Members," 75 *Federal Register* 7 (January 12, 2010), pp 1595-1596. https://federalregister.gov/a/2010-344

National Institute of Standards and Technology (December 2002) *Security Requirements for Cryptographic Modules*, December 2002. https://doi.org/10.6028/NIST.FIPS.140-2.

International Organization for Standardization, International Electrotechnical Commission (June 2011) *Information technology—Security techniques—Information security risk management*, June 2011. ISO/IEC 27005:2011. URN urn:iso:std:iso-iec:27005:stage-95.99:ed-2. https://www.iso.org/standard/56742.html.

National Institute of Standards and Technology (2018) *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018 [NIST CSF]

Paulsen C, Boyens J, Bartol N, Winkler K (April 2018) *Criticality analysis process model: prioritizing systems and components* (National Institute of Standards and Technology, Gaithersburg, MD), NIST NISTIRs (Interagency/Internal Reports) (IR) 8179, April 2018. https://doi.org/10.6028/NIST.IR.8179.

D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk (May 2008) *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* RFC 5280, May 2008. IETF RFC 5280. DOI 10.17487/RFC5280. https://www.rfc-editor.org/info/rfc5280.

Dr. Ron S. Ross, Kelley L. Dempsey, Patrick Viscuso, Mark Riddle, Gary Guissanie (June 2018 (updated June 2018)) *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, June 2018 (updated June 2018). https://doi.org/10.6028/NIST.SP.800-171r1.

Scott W. Rose, Stephen Nightingale, Simson L. Garfinkel, Ramaswamy Chandramouli (September 2016) *Trustworthy Email*, September 2016. https://doi.org/10.6028/NIST.SP.800-177.

Jeffrey A. Cichonski, Joshua M. Franklin, Michael Bartock (December 2017) *Guide to LTE Security*, December 2017. https://doi.org/10.6028/NIST.SP.800-187.