kantara INITIATIVE

Ruth Puente <ruth@kantarainitiative.org>

[SG-800-63-3] Preliminary work on 63-3B

Andrew Hughes <andrewhughes3000@gmail.com> Wed, Aug 23, 2017 at 11:53 AM
To: sg-800-63-3@kantarainitiative.org

Hi folks - I've been making some progress on transforming the 63B text this week.

I have been thinking about what kinds of markup, metadata, manipulation and presentation activities that Kantara will need to do with the future publication.

We desperately need to have some structured text to work with - call it a database, spreadsheet or whatever. Structural elements will allow for filtering, selective output and output into any needed file format.

So.

As a test, I have taken the 800-63-3B markdown files from the NIST github repo and loaded them into an authoring tool and applied a DocBook 5 styler.

The screenshots you see are from that tool, XMLMind.

The green text is the original NIST text, unmodified.
The blue text is the "Kantara" version - in many cases there are no modifications. You will see some of the NIST sentences which contain multiple requirements or funky conditionals, broken out into single requirements. Sometimes the extra words are removed, etc.

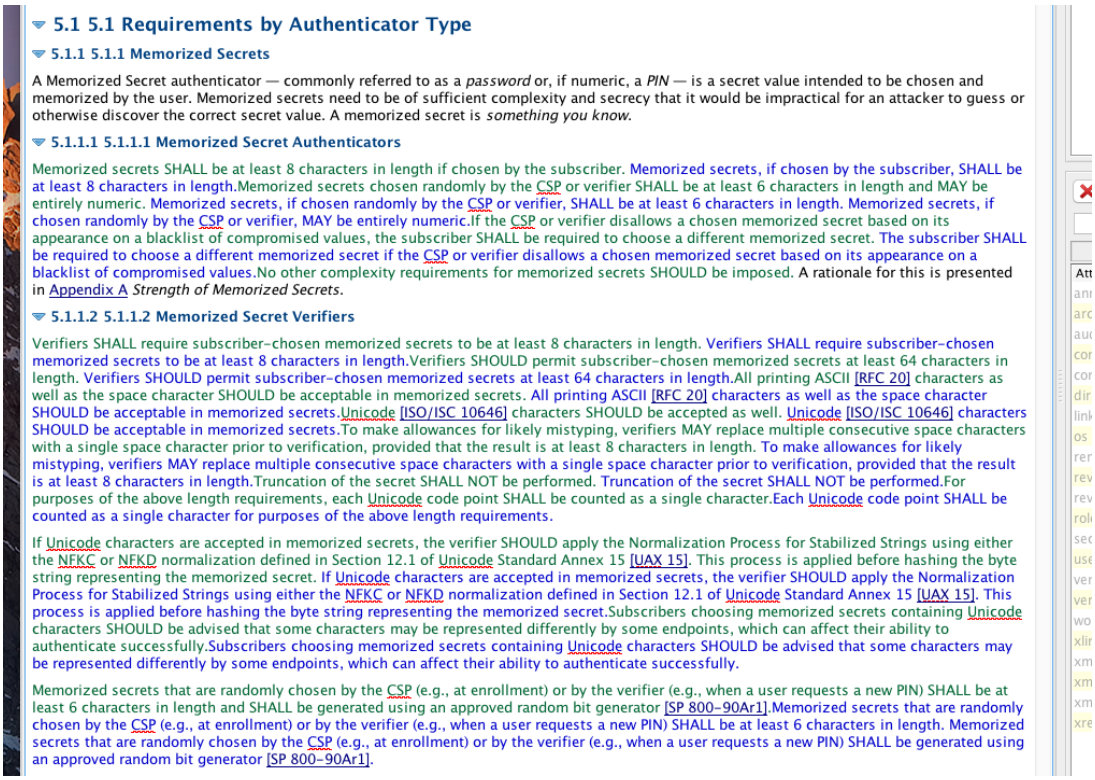
I have used a metadata structure that includes the optionality, and other tags to make future filtering and extraction for different audiences possible.

You will see that I tagged every requirement including the optional SHOULD/MAY ones for completeness - these are simple to filter out if we only want the SHALL statements.

With this structure, we can easily generate unique requirements names a naming convention; link directly back to the original NIST text; add notes; provide links to external pages and documents; generate HTML/PDF/DOCX/CSV/Markdown versions; add whatever metadata we want to create different versions.

The conversion from markdown into DocBook isn't too painful - and in fact, if we do go down this path, offering the DocBook version of the original text (minus the Kantara customizations) back to NIST might be on the table.

Version showing NIST and Kantara text:



5.1 5.1 Requirements by Authenticator Type

5.1.1 5.1.1 Memorized Secrets

A Memorized Secret authenticator — commonly referred to as a *password* or, if numeric, a *PIN* — is a secret value intended to be chosen and memorized by the user. Memorized secrets need to be of sufficient complexity and secrecy that it would be impractical for an attacker to guess or otherwise discover the correct secret value. A memorized secret is *something you know.*

5.1.1.1 5.1.1.1 Memorized Secret Authenticators

Memorized secrets SHALL be at least 8 characters in length if chosen by the subscriber. Memorized secrets, if chosen by the subscriber, SHALL be at least 8 characters in length.Memorized secrets chosen randomly by the CSP or verifier SHALL be at least 6 characters in length and MAY be entirely numeric. Memorized secrets, if chosen randomly by the CSP or verifier, SHALL be at least 6 characters in length. Memorized secrets, if chosen randomly by the CSP or verifier, MAY be entirely numeric.If the CSP or verifier disallows a chosen memorized secret based on its appearance on a blacklist of compromised values, the subscriber SHALL be required to choose a different memorized secret. The subscriber SHALL be required to choose a different memorized secret if the CSP or verifier disallows a chosen memorized secret based on its appearance on a blacklist of compromised values.No other complexity requirements for memorized secrets SHOULD be imposed. A rationale for this is presented in Appendix A *Strength of Memorized Secrets*.

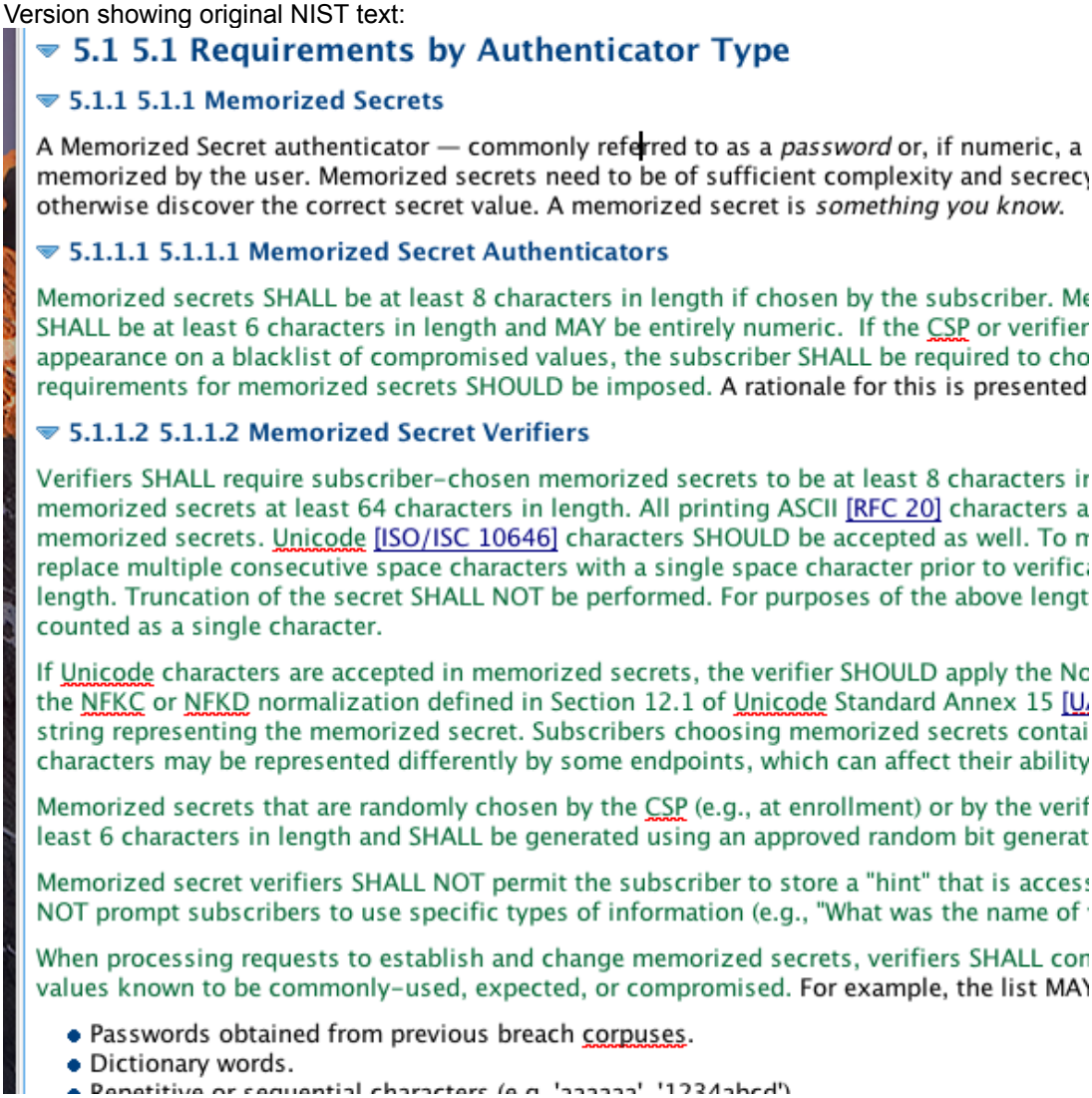
5.1.1.2 5.1.1.2 Memorized Secret Verifiers

Verifiers SHALL require subscriber-chosen memorized secrets to be at least 8 characters in length. Verifiers SHALL require subscriber-chosen memorized secrets to be at least 8 characters in length.Verifiers SHOULD permit subscriber-chosen memorized secrets at least 64 characters in length. Verifiers SHOULD permit subscriber-chosen memorized secrets at least 64 characters in length.All printing ASCII [RFC 20] characters as well as the space character SHOULD be acceptable in memorized secrets. All printing ASCII [RFC 20] characters as well as the space character SHOULD be acceptable in memorized secrets.Unicode [ISO/ISC 10646] characters SHOULD be accepted as well. Unicode [ISO/ISC 10646] characters SHOULD be acceptable in memorized secrets.To make allowances for likely mistyping, verifiers MAY replace multiple consecutive space characters with a single space character prior to verification, provided that the result is at least 8 characters in length. To make allowances for likely mistyping, verifiers MAY replace multiple consecutive space characters with a single space character prior to verification, provided that the result is at least 8 characters in length.Truncation of the secret SHALL NOT be performed. Truncation of the secret SHALL NOT be performed.For purposes of the above length requirements, each Unicode code point SHALL be counted as a single character.Each Unicode code point SHALL be counted as a single character for purposes of the above length requirements.

If Unicode characters are accepted in memorized secrets, the verifier SHOULD apply the Normalization Process for Stabilized Strings using either the NFKC or NFKD normalization defined in Section 12.1 of Unicode Standard Annex 15 [UAX 15]. This process is applied before hashing the byte string representing the memorized secret. If Unicode characters are accepted in memorized secrets, the verifier SHOULD apply the Normalization Process for Stabilized Strings using either the NFKC or NFKD normalization defined in Section 12.1 of Unicode Standard Annex 15 [UAX 15]. This process is applied before hashing the byte string representing the memorized secret.Subscribers choosing memorized secrets containing Unicode characters SHOULD be advised that some characters may be represented differently by some endpoints, which can affect their ability to authenticate successfully.Subscribers choosing memorized secrets containing Unicode characters SHOULD be advised that some characters may be represented differently by some endpoints, which can affect their ability to authenticate successfully.

Memorized secrets that are randomly chosen by the CSP (e.g., at enrollment) or by the verifier (e.g., when a user requests a new PIN) SHALL be at least 6 characters in length and SHALL be generated using an approved random bit generator [SP 800-90Ar1].Memorized secrets that are randomly chosen by the CSP (e.g., at enrollment) or by the verifier (e.g., when a user requests a new PIN) SHALL be at least 6 characters in length. Memorized secrets that are randomly chosen by the CSP (e.g., at enrollment) or by the verifier (e.g., when a user requests a new PIN) SHALL be generated using an approved random bit generator [SP 800-90Ar1].

Version showing original NIST text:



5.1 5.1 Requirements by Authenticator Type

5.1.1 5.1.1 Memorized Secrets

A Memorized Secret authenticator — commonly referred to as a *password* or, if numeric, a memorized by the user. Memorized secrets need to be of sufficient complexity and secrecy otherwise discover the correct secret value. A memorized secret is *something you know.*

5.1.1.1 5.1.1.1 Memorized Secret Authenticators

Memorized secrets SHALL be at least 8 characters in length if chosen by the subscriber. Me SHALL be at least 6 characters in length and MAY be entirely numeric. If the CSP or verifier appearance on a blacklist of compromised values, the subscriber SHALL be required to cho requirements for memorized secrets SHOULD be imposed. A rationale for this is presented

5.1.1.2 5.1.1.2 Memorized Secret Verifiers

Verifiers SHALL require subscriber-chosen memorized secrets to be at least 8 characters ir memorized secrets at least 64 characters in length. All printing ASCII [RFC 20] characters a memorized secrets. Unicode [ISO/ISC 10646] characters SHOULD be accepted as well. To m replace multiple consecutive space characters with a single space character prior to verific length. Truncation of the secret SHALL NOT be performed. For purposes of the above lengt counted as a single character.

If Unicode characters are accepted in memorized secrets, the verifier SHOULD apply the No the NFKC or NFKD normalization defined in Section 12.1 of Unicode Standard Annex 15 [U string representing the memorized secret. Subscribers choosing memorized secrets contai characters may be represented differently by some endpoints, which can affect their ability

Memorized secrets that are randomly chosen by the CSP (e.g., at enrollment) or by the verif least 6 characters in length and SHALL be generated using an approved random bit generat

Memorized secret verifiers SHALL NOT permit the subscriber to store a "hint" that is acces NOT prompt subscribers to use specific types of information (e.g., "What was the name of

When processing requests to establish and change memorized secrets, verifiers SHALL cor values known to be commonly-used, expected, or compromised. For example, the list MA

- Passwords obtained from previous breach corpuses.
- Dictionary words.
- Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd')

Version showing only Kantara text:

5.1 5.1 Requirements by Authenticator Type

5.1.1 5.1.1 Memorized Secrets

A Memorized Secret authenticator — commonly referred to as a *password* or, if numeric, a *PIN* — is a secret value intended to be chosen and memorized by the user. Memorized secrets need to be of sufficient complexity and secrecy that it would be impractical for an attacker to guess or otherwise discover the correct secret value. A memorized secret is *something you know.*

5.1.1.1 5.1.1.1 Memorized Secret Authenticators

Memorized secrets, if chosen by the subscriber, SHALL be at least 8 characters in length.Memorized secrets, if chosen randomly by the CSP or verifier, SHALL be at least 6 characters in length. Memorized secrets, if chosen randomly by the CSP or verifier, MAY be entirely numeric.The subscriber SHALL be required to choose a different memorized secret if the CSP or verifier disallows a chosen memorized secret based on its appearance on a blacklist of compromised values.A rationale for this is presented in Appendix A *Strength of Memorized Secrets*.

5.1.1.2 5.1.1.2 Memorized Secret Verifiers

Verifiers SHALL require subscriber-chosen memorized secrets to be at least 8 characters in length.Verifiers SHOULD permit subscriber-chosen memorized secrets at least 64 characters in length.All printing ASCII [RFC 20] characters as well as the space character SHOULD be acceptable in memorized secrets.Unicode [ISO/ISC 10646] characters SHOULD be acceptable in memorized secrets.To make allowances for likely mistyping, verifiers MAY replace multiple consecutive space characters with a single space character prior to verification, provided that the result is at least 8 characters in length.Truncation of the secret SHALL NOT be performed.Each Unicode code point SHALL be counted as a single character for purposes of the above length requirements.

If Unicode characters are accepted in memorized secrets, the verifier SHOULD apply the Normalization Process for Stabilized Strings using either the NFKC or NFKD normalization defined in Section 12.1 of Unicode Standard Annex 15 [UAX 15]. This process is applied before hashing the byte string representing the memorized secret.Subscribers choosing memorized secrets containing Unicode characters SHOULD be advised that some characters may be represented differently by some endpoints, which can affect their ability to authenticate successfully.

Memorized secrets that are randomly chosen by the CSP (e.g., at enrollment) or by the verifier (e.g., when a user requests a new PIN) SHALL be at least 6 characters in length. Memorized secrets that are randomly chosen by the CSP (e.g., at enrollment) or by the verifier (e.g., when a user requests a new PIN) SHALL be generated using an approved random bit generator [SP 800-90Ar1].

Memorized secret verifiers SHALL NOT permit the subscriber to store a "hint" that is accessible to an unauthenticated claimant.Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing memorized secrets.

When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised.For example, the list MAY include, but is not limited to:

Andrew Hughes CISM CISSP
Independent Consultant
In Turn Information Management Consulting

o +1 650.209.7542
m +1 250.888.9474
1249 Palmer Road,
Victoria, BC V8P 2H8
AndrewHughes3000@gmail.com
ca.linkedin.com/pub/andrew-hughes/a/58/682/
Identity Management | IT Governance | Information Security
