Questions

Overall

Q There is no functionality present for managing identities in the IdentityStore, e.g. for allowing new users to sign up in an application and for having authorizations given or withdrawn from within an application. Is this foreseen for a future version, or will this be left to non-standard extensions?

Q Chapter 3 mentions user groups, and chapter 4 mentions roles for users – however the relationship between these two concepts is not described anywhere. Should the mechanism by which this relation (i.e. users/groups mapping to roles/permissions) is configured be standardized too, or will this be left to non-standard extensions?

Chapter 1 – Concepts

Q Why is the list, as proposed on the java.net project page, not used here as a starting point?

Q Add terms/abbreviations that are frequently used on the mailing list? E.g. SAM, HAM.

Chapter 2 – Authentication Mechanism

Q Will the HttpAuthenticationMechanism (or a similar) interface become available for other inbound traffic handling container types? If not, why not?

Section 2.1 – Introduction

Q "… through the process of authentication": isn't this step actually called identification? (and, as stated correctly afterwards, authentication is the presenting of proof of identity)

Section 2.2 – Interface and Theory of Operation

Q The last method is called cleanSubject(), yet the term "subject" isn't used anywhere else in the specification. Can another, already used term be applied here as well, or is it a significantly different entity?

Q How do the calls to these methods fit in the lifecycle of a client session? Could this be illustrated in the specification?

Section 2.3 – Installation and Configuration

Q Would it be clearer what is meant by "enabled bean" and "normal scoped" by referring to the defining sections in CDI specification?

Q Why is it not specified how the configuration over which mechanism is to be done?

Chapter 3 – Identity Store

Q The concept of multiple identity stores is introduced, but are there restrictions that should apply to each single store? Such as uniqueness of each identity entry within that store, or at least consistency of which entry is used for validation or returning groups for upon a given enquiry?

Section 3.2.1 – Validating Credentials

Q Wouldn't it be better to indicate the validate() method as MANDATORY for IdentityStores that declare themselves to have AUTHENTICATION or BOTH capability (instead of OPTIONAL)?

Questions

Q Instead of providing a status value (or called “error code” in the review section), shouldn’t the signature of the method indicate that specific exceptions can be thrown in exceptional cases (such as the failure causes mentioned in the review section)

Section 3.2.2 – Retrieving Caller Information

Q Wouldn’t it be better to indicate the getGroupsByCallerPrincipal() method as MANDATORY for IdentityStores that declare themselves to have AUTHORIZATION or BOTH capability (instead of OPTIONAL)?

Section 3.2.4 – Handling Multiple Identity Stores

Q How are different Credentials, spread over multiple identity stores, for the same user correlated with a single CallerPrincipal (which currently only contains a ‘name’ field)? How can it be prevented that Credentials for different users are correlated to the same CallerPrincipal? How can such consistency be enforced (or even be maintained)?

Q Shouldn’t the remark made in section 3.3, that equal priorities lead to an undefined calling order, be moved to this section? It seems more appropriate here.

Q The reasoning behind *why* the identity stores are filtered for the two steps is missing (or implicit) from the process description. What is it, and should it be added to the section for clarification?

Q Shouldn’t the case where no VALID response was received, but errors did occur (as described in the third bullet of the review section), result in an exception being thrown?

Section 3.3 – Installation and Configuration

Q Ad review section: Isn’t it confusing or possibly even just wrong to accept group data from an authentication-only identity store? Isn’t it so that the validation type is under the control of the application, while the process/implementation through which the group data is returned from such a store may not be?

Section 3.4 – Annotations and Built-in IdentityStore Beans

Q What is the reasoning behind the various default values for priority() as used in the annotations? Why is the order defined like this?

Section 4.4 – Relationship to Other Specifications

Q Would it be a goal to have the existing ‘alternatives’ in the other specifications be deprecated for Java EE 9?

Typos

Section 2.1 – Introduction	In the third paragraph, first line: “… the iteraction...” should be “… the i**n**teraction...”
	Third paragraph, third line: “… the construction an...” should be “… the construction **of** an…”
Section 2.2 – Interface and Theory of Operation	Page 5, summary of cleanSubject(): “… the logout method...” should be “… the logout**()** method...”
	Page 5, paragraph directly after the summary: redundant use of “for example” (twice), where “etc.” of “such as...” is used
Section 2.4 – Relationship to other specifications	Second paragraph, third line: “… method of servlet filter…” should be “… method of **a** servlet filter...”
	Second paragraph, fifth line: “… validateRequest…” should be “… validateRequest**()**...”
	Third paragraph, first line: “… build-in...” should be “… buil**t**-in…”
Section 3.1 – Introduction	Third paragraph: “A primary advantage...” should be “**The** primary advantage...”(?)
	Fourth paragraph, second line: “… passed in to it...” should be “… passed **into** it...”
Section 3.2.1 – Validating Credentials	Page 9, section under review section: missing _ before “validate(Credential)_” to make it italic
Section 3.2.4 – Handling Multiple Identity Stores	Second paragraph, fourth line: “… qualier…” should be “… quali**fi**er...”
	Page 12, one-but-last line: “… passed in to this method...” should be “… passed **into** this method…”
Section 3.4 – Annotations and Built-in IdentityStore Beans	Page 15, mid-way: “All of ~~all~~ these beans...” should be “All of these beans...”
Chapter 4 – Security Context	Various instances on pages 17 and 18: “SecurityContect” should be “SecurityConte**x**t”
Section 4.2 – Testing for Caller Data	Last paragraph, second line: “… role determinatino...” should be “… role determinati**on**...”