1.0 [Assertion] Basic Info, Conditions, and Advice: [aka "Header"]

[Clairfying discussion about these questions'n'arrows appears in the minutes in section I.6.0, and in section II. Nominally, there were proposals for moving "audience" up to a first-class element of the Header, and for moving the validity interval info (NotBefore & NotOnOrAfter) down into conditions. ed.]

[a] = Optional. May appear in various font sizes.

[ ] = Struct

{ } = Union

Text in bold = an issue. Issues were in BROWN on the whiteboards. (BROWN text and/or symbols signified things that the group wasn't confident about and/or that was contentious (stuff we were relatively confident about was written in orange (on the whiteboards, not in these notes). Note that some editorial comments may be issues, see below)

? = Big, bold question mark -- an issue, may or may not be accompanied by text in bold

? = Non-bold question mark -- hmm, more to think about here. Is this an issue?


* = Repetition 0..n If it was written in BROWN on the whiteboard, it is explicitly noted in this document.

+ = Repetition 1..n

= Callout. If callout text is in [brackets], then callout is an editorial comment. Else callout appeared on the whiteboard, and if text is bold, then it was written in BROWN.

"the minutes" = http://www.oasis-open.org/committees/security/minutes/SSTC-F2F-3-Minutes-00.txt
2.0. Authentication Assertion
Source: http://www.oasis-open.org/committees/security/minutes/SSTC-F2F-3-whiteboard-1a-big.jpg

2.1. The types of queries/requests we need to make for Authentication Assertions
Source: same as 2.0.

(1) Return (#) unexpired authn assertions for "this" subject. [via authntype (#)?]

(2) Return the authn assertion with assnId (#).

2.2. Request message for obtaining an Authentication Assertion
Source: same as 2.0.
[implication is that one must be able to use this message to pose both of the queries in 2.1. ed.]

[As noted in the minutes in ISSUE:[F2F#3-35], BobB indicated he has some comments on the use of "bearer" and where it is and isn't appropriate in the various Assertions and their respective Req/Response messages. ed.]

[These questions were nominally decided. See the minutes, section I.4.0 on composition of AuthnType ed.]

[Note that this repetition indicator was in BROWN. ed.]
2.3. Response message to Authentication Assertion request message
Source: same as 2.0.

RSP:

```
assertion *
status code
```

3.0. Attribute Assertion
Source: http://www.oasis-open.org/committees/security/minutes/SSTC-F2F-3-whiteboard-1b-big.jpg

Attribute Assertion Info:

- Attr Name
- Attr value
- Security Domain Name
  - bearer
  - h.o.k.
  - assnid (assertion?)

[We didn't include "Header" here, in the text on the whiteboard. I presume we do want it. ed.]

[I.e. "holder of key". This item was circled in BLUE. Significance? ed.]

[These angle brackets were written in BROWN. Use of xmlns indicator here needs more discussion. See ISSUE:[F2F#3-27]. ed.]

[There was much discussion about Attr values. See the minutes sections III and IV, and ISSUE:[F2F#3-28], ISSUE:[F2F#3-29]. ed.]

[see (at least) ISSUE:[F2F#3-19], ISSUE:[F2F#3-26], ISSUE:[F2F#3-27] in section IV of the minutes. ed.]
3.1. The types of queries/requests we need to make for Attribute Assertions

Source: same as 3.0.

Q: (1) Give me all the attributes for the subject (#)

ANY | ALL.

(2) Give me the following attributes (#) for the Subject (#)

(3) Return the attribute assertion with assnid (#)

(4) Give me the names of attributes the following Subject (#) has (not their values) ? (Solicit use case)

3.2. Request message for obtaining Attribute Assertion(s)

Source: same as 3.0.

[implication is that one must be able to use this message to pose all of the queries listed in 3.1. ed.]

3.3. Response message to Attribute Assertion request message

Source: same as 3.0.

[Note that this was circled in BLUE. ed.]
4.0. Authorization Decision Assertion  
Source: http://www.oasis-open.org/committees/security/minutes/SSTC-F2F-3-whiteboard-2-big.jpg

We didn't include "Header" here, in the text on the whiteboard. I presume we do want it. ed.

[Authorization Decision Assertion] [Info:] [Header]

Subject spec.  
<subject assertions>
object
action
answer (Y/N/-?)

[Security Domain Name]
bearer
(assnid/assertion)*

[The same questions apply in both of these places. See at least: ISSUE:[F2F#3-30], ISSUE:[F2F#3-31] ed.]

4.1. The types of queries/requests we need to make for Authorization Decision Assertions  
Source: same as 4.0.

Q's (1) Should action Y on object Z be allowed given evidence E (including subject & optionally subject assertions)

4.2. Request message for obtaining Authorization Decision Assertion  
Source: same as 4.0.

RQ:  
Subject specifier
<subject assertions>
object
action
assnid | assertion

Security domain name
bearer
registry of namespaces?

do subj. assertions have to be assertions about the same Subject as the one in the subj. specifier.

[?] [see sections V.3.0 and VI of the minutes. ed.]

[Note that this repetition indicator was in BROWN. There's open questions about what having assnids here constitutes semantically. Advice? see sections V.3.0 and VI of the minutes, and ISSUE:[F2F#3-33], ISSUE:[F2F#3-34] ed.]
4.3. Response message to Authorization Decision request message
Source: same as 4.0.

RSP: assertion
    status code

End of document.