1. [Assertion] Basic Info [aka "Header"]

source: http://www.oasis-open.org/committees/security/minutes/SSTC-F2F-3-whiteboard-2-big.jpg

[Actually, we didn’t draw a struct indicator around this set of items. Should we have? ed.]

Basic Info [aka "Header"]
- Version
- AssertionID
- Issuer
- Issue Instant
  - NotBefore
  - NotOnOrAfter
- Conditions
  - Audience
- Advice

[This one question mark of the three here was the only one in BROWN. ed.]

[What was our discussion involving all these arrows & question marks?? ed.]
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.

Q:
(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.]
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:

```
[Header]

Subject

Attr Name
<xmlns>

Attr value

+ Security Domain Name
  bearer
  h.o.k.

asnid (assertion?)
```

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

[These angle brackets were written in BROWN. Use of xmlns indicator here needs more discussion. 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 (#)
   (not other?)

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

(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.

RSP: [assertion *

status code
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]

Security Domain Name
bearer
(assnid/assertion)*

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

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:

Security domain name
bearer
assertionID | assertion

subject specifier
<subject assertions>
object
action
assnid *

URI
namespace
actionname

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

[?] registry of namespaces?

[Note that this repetition indicator was in BROWN. ed.]
4.3. Response message to Authorization Decision request message
Source: same as 4.0.

RSP: [assertion
status code]

End of document.