Introduction para 2 - what we are saying here is about Authentication – but the term isn't used. Given that this is such a commonly used term in the security community, its use would be helpful to set the expectations of the audience

Introduction para 3:

- Is our aim really to produce a document that "specifies the necessary metadata" – isn't that being too specific? Aren't we about the processes that should be supported
- Not sure about "…allows signatures to be shared among applications to ensure the integrity and a means for …". We aren't really interested in sharing signatures – that's a side effect of what we are actually doing. What we are actually doing is ensuring that source code can be unique identified
- "reversing the application of the signatures" We're not really reversing the signature, we are permitting the roll-back to previously signed versions

Section 1: Scope

- "…define the methodology needed to support the signing of software source code." As this is the first real section of the document (I don't think you can count the introduction), I think the purpose should be repeated here, e.g. '… source code, to enable it to be uniquely identified, and to enable roll-back to previous signed versions'
- Whilst the exclusion of the third bullet "Digital signing of object or binary code" is in line with what we've talked about to date, it is a real issue – and this standard would be a lot more useful it is provided a solution to the problem of ensuring the that the source code you've tested and certified is actually the source of the program being run:
    - Could we add an 'implication for standardization', along the lines we've added in the main body, such as 'if a compiler is processing source code with a digital signature, that signature shall be embedded in, and recoverable from the resulting executable'

Section 2: Conformance - para 2

- (may have been covered in the meeting) "Clause 5 provides an overview of the concepts of code signing. Annex A is informative and provides a possible scenario of usage for the standard specified in Clause 6." This isn't about Conformance and should be in Scope or Introduction

Section 4: Terms and definitions

- In general, whilst there are lots of good terms in here, I think we need to wait until the later sections are agreed, and then only provide definitions for terms used – I think there are terms here that are a throwback to when the standard was to be more prescriptive
- 4.12 – a snapshot doesn't need to be a verbatim copy – it just needs you to be able to restore to the same state. I can take a snapshot by creating a ZIP archive – that's not a verbatim copy of the original

Section 5: Concepts

First bulleted list

- Fifth bullet is a repeated sentence

Second bulleted list

- First bullet "a tracking mechanism to show what has been altered in the source code and by whom" – whilst this was what we initially talked about, I'm not sure it's still the intent. From the objectives and scope, I don't see where we've said anything about who has changed what – merely that you can get back to a previously signed state

Section 6.4 – last para

- Same as comment immediately above "…and a record of all changes that distinguish any signed version from any preceding signed version" I think this means metadata to record changes – saying you can recover the original source and use a third party diff tool to find the changes sounds like cheating
- This issue is also reflected in 6.5 "This International Standard is not prescriptive as to which format shall be used to create or track revisions" – but it sounds like we are expecting data to be added