Q1: **Clarity** – Are the descriptions of the concerns clear and unambiguous? Would you suggest any modification?

The descriptions are clear. I suggest to take into account saying what the user must show, to whom, for how long and what happens if the system fails or is unsure. You could also consider for Transparency to show a short refusal message that who have not the requested age can understand and act on. You could also name some actual security threats (like spoofing, social engineering) to frame the concerns to reality.

Q2: **Relevance** – Are the concerns relevant in the context of age verification systems? Would you remove any of them?

All the concerns fit, Trust and Social Acceptance should be relevant also as an evidence-supported outcome. You could also consider that the age check can happen in public or shared settings so "doxing", shame, coercion should also be avoided in public contexts.

Q3: **Actionability** – Can these concerns realistically be addressed in age verification systems?

Yes, as long as age verification will not turn in a permanent identification, retaining information for minutes or hours and not "as short as possible".

Q4: **Completeness** – Are these concerns comprehensive to address the ethical aspects of age verification systems? Would you include others?

The concerns could also include: (i) time-sensitive retention, the proof should fade quickly to not become a trace; (ii) coercion resilience to keep the user safe; (iii) unlinkability and revocation so the pass cannot be reused for tracking; (iv) vendors incentives measured by user protection (low data use, fast appeals, few denials) and not by retained data; (v) accessibility can be a concern in terms of language, bad connectivity, device, as age verification should not be an obstacle.