|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| KI/SS |  |  |  | Ge | Most of the document is a section called “privacy enhancing services” that mostly contains various authentication functions.  There’s a brief section on pseudonymous attributes, but otherwise most of the contents of that section are not really about privacy.  Authentication is a function that enables other security functions like access control, which THEN enable good privacy settings if managed correctly.  That doesn’t mean that regular authentication is a privacy function.  It frequently references the problem without necessarily offering any guidance on its solution. Some examples - the section “identity authentication” discusses the privacy properties of civil identification / identity proofing, but provides nothing about how to make the decision, communicate the decision to others who might need to know (e.g. how do relying parties know if ICC credentials were issued based on pseudonymous identifiers) or otherwise how ICC-based systems should implement such privacy controls.    There’s decent discussion of protecting attributes disclosure using the COMPARE command in section 7.4 but then it “solves” the problem by saying “use privacy enhancing protocols and access control to do the right thing”.  I’m following the circular reasoning around and not getting anywhere.    Part of the problem seems that it does not identify the audience.  It frequently references the problem without necessarily offering any guidance on its solution.    Some examples - the section “identity authentication” discusses the privacy properties of civil identification / identity proofing, but provides nothing about how to make the decision, communicate the decision to others who might need to know (e.g. how do relying parties know if ICC credentials were issued based on pseudonymous identifiers) or otherwise how ICC-based systems should implement such privacy controls.    That said, the content could be directed towards smart cards, where their function is basically authentication and the privacy concerns are mostly related to leaking PII, particularly without authentication.  So to some extent the focus makes sense, if that is the case. But it was far from clear upon reading it. | No specific proposals can be made because the audience and the scope is not clear.  Suggest that ITTF undertakes some re-consideration of the Introduction and Scope sections to improve these aspects. |  |
|  |  |  |  |  |  |  |  |