We propose a set of requirements for the WebRTC signaling protocol that 3GPP defines:

* It should not overfit for specific use case.
* It shall enable communicating parties to match based on
  + Flexible matching with a wide range of matching criteria that suit the needs of different WebRTC applications.
  + Secure matching to avoid security issues such as DDoS attacks
  + Global matching possibilities for applications that work across multiple WebRTC signaling servers, potentially hosted by different MNOs.
* It shall enable communicating parties to verify each other’s identity, if required by the application.
* It shall support the secure exchange of messages supporting integrity-protection and/or encryption.
* It shall protect user privacy and mitigate the linkability and tracking attack caused by unnecessary user information disclosure.
  + Note: detailed security requirements and mechanisms need further co-work with SA3.
* It shall support basic session setup messages allowing extension for application-specific information.
* It should be web-friendly to support easy deployment in web applications
  + It should use web technologies such as JSON, WebSockets, etc…
  + It shall comply with WebRTC standards (e.g., SDP for session description and supporting the exchange of ICE candidates, etc…) defined in IETF and W3C except for codecs
* It shall be simple to implement and deploy.