

## Privacy Browser - Feature #210

### Specify Privacy WebView's SSL settings

09/28/2017 11:39 PM - bill bunter

<b>Status:</b>	New	<b>Start date:</b>	09/28/2017
<b>Priority:</b>	4.x	<b>Due date:</b>	
<b>Assignee:</b>	Soren Stoutner	<b>% Done:</b>	0%
<b>Category:</b>		<b>Estimated time:</b>	0.00 hour
<b>Target version:</b>		<b>Spent time:</b>	0.00 hour
<b>Description</b>			
If you included open SSL in privacy browser would that allow to for user to disable weak TLS ciphers that are still in the Android open SSL on older phones? And even to specify cipher suite to be used in Domain pinning?			

#### History

##### #1 - 09/29/2017 12:09 AM - Soren Stoutner

- Subject changed from ssl library to Specify Privacy WebView's SSL settings
- Assignee changed from bill bunter to Soren Stoutner
- Priority changed from 2 to 3.x

Shipping an SSL library with Privacy Browser would probably require too much time to implement correctly and opens up the possibility of introducing more bugs than it fixes. Plus it has all the downsides listed below.

It is possible to manually specify what settings are used with the SSL library already included in Android using `HttpsURLConnection`, `SSL Engine`, `SSL Socket Factory`, and `SSL Parameters`. However, to integrate this with `WebView` would require making all data requests manually, processing them myself, and feeding them into `WebView`, a process that is likely to introduce a massive number of bugs.

<https://developer.android.com/reference/javax/net/ssl/HttpsURLConnection.html>

<https://developer.android.com/reference/javax/net/ssl/SSL Engine.html>

<https://developer.android.com/reference/javax/net/SocketFactory.html>

<https://developer.android.com/reference/javax/net/ssl/SSLParameters.html>

With the introduction of Privacy WebView, it should be possible to modify the SSL settings in WebView without having to re-implement all the these other aspects. However, it will likely be a couple of years before the 4.x series is released.

<https://www.stoutner.com/category/roadmap/>

##### #2 - 11/06/2017 07:33 PM - Soren Stoutner

- Priority changed from 3.x to 4.x