The problem of SSL/TLS interception („trusted proxy in SSL/TLS connection“) has been known for years and many implementations exist. However, all of them share a single technical solution which is based solely on the PKI authentication mechanism and suffers from multiple serious disadvantages. Most importantly, it is not compatible with several aspects or future trends of SSL/TLS and PKI, there's almost no space for improvement and its real use may spawn legal issues. After we analyze technical background and the current solution, we will propose another one, based not only on PKI but SSL/TLS too. Both solutions will be compared and general superiority of the new one will be shown. Basic implementation and analysis will follow, along with deployment requirements and ideas for future development.