Sequence of actions when Alice logs in using certificate based login:

|  |  |
| --- | --- |
| **ALICE** | **SERVER** |
| *Authentication* | |
| Login request cert based |  |
| Send get nonce |  |
|  | Generate random nonce Ns |
|  | Return Ns to Alice |
| Send EP-ALICE(Ns) |  |
|  |  |
|  |  |