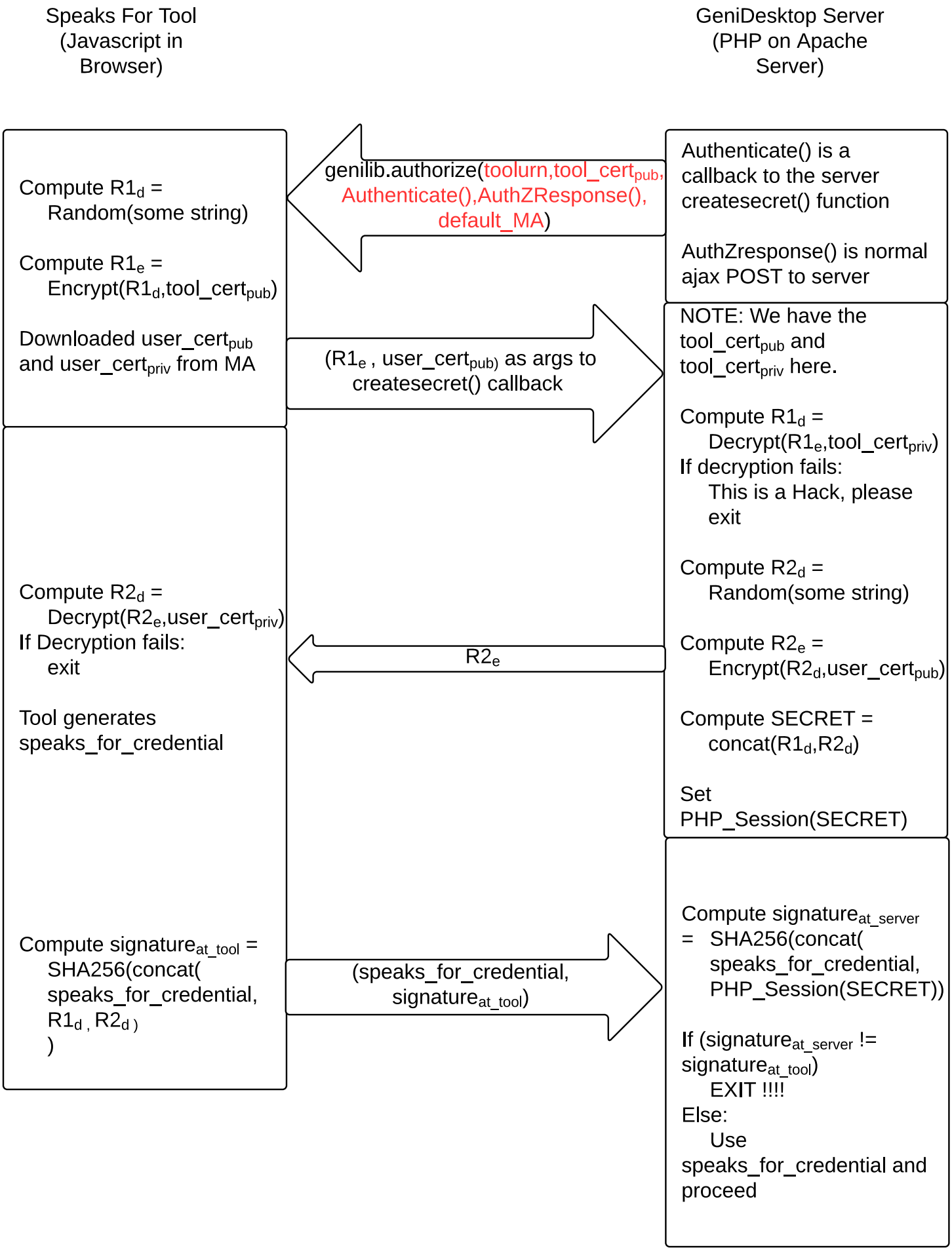
Speaks For Tool (Javascript in Browser)
GeniDesktop Server (PHP on Apache Server)
Compute R1d = Random(some string)
Compute R1e = Encrypt(R1d,tool_certpub)
Downloaded user_certpub and user_certpriv from MA
genilib.authorize(toolurn,tool_certpub, Authenticate(),AuthZResponse(), default_MA)
Authenticate() is a callback to the server createsecret() function
AuthZresponse() is normal ajax POST to server
(R1e , user_certpub) as args to createsecret() callback
NOTE: We have the tool_certpub and tool_certpriv here.
Compute R1d = Decrypt(R1e,tool_certpriv)
If decryption fails:
This is a Hack, please exit
Compute R2d = Random(some string)
Compute R2e = Encrypt(R2d,user_certpub)
Compute SECRET = concat(R1d,R2d)
Set PHP_Session(SECRET)
R2e
Compute R2d = Decrypt(R2e,user_certpriv)
If Decryption fails:
exit
Tool generates speaks_for_credential
Compute signature at_tool = SHA256(concat(speaks_for_credential, R1d , R2d))
(speaks_for_credential, signature at_tool)
Compute signature at_server = SHA256(concat(speaks_for_credential, PHP_Session(SECRET))
If (signature at_server != signature at_tool)
EXIT !!!!
Else:
Use speaks_for_credential and proceed