Allowing SNI in the CertificateRequest is changing TLS 1.3 by allowing the SNI extension (requires UPDATES RFC 8446)

- Recall: the client-initiated exported authenticator flow starts with an authenticator request (containing a CertificateRequest-like structure) generated on the client.

**Extensions:** The extensions that are allowed in this structure include the extensions defined for CertificateRequest messages defined in Section 4.2. of [TLS13] and the server_name [RFC6066] extension, which is allowed for client-generated authenticator requests.
Proposals

a) Change the document to UPDATE RFC 8446

b) Ask for a new extension point for SNI sent in a client-generated authenticator request.

c) Treat the CertificateRequest-like structure in client-generated exported authenticator requests like a **ClientHello** when generated by the client. Specifically, allow CH-extensions when client-generated and allow CR-extensions when server-generated.
extensions:
- The extensions that are allowed in this structure include the extensions defined for CertificateRequest messages defined in Section 4.2. of {{!TLS13}} and the server_name {{!RFC6066}} extension, which is allowed for client-generated authenticator requests.
+ In the case of server-generated authenticator requests, the set of extensions allowed in this structure are those defined in the TLS ExtensionType Values IANA registry containing CR in the TLS 1.3 column. For client-generated authenticator requests, the set of extensions allowed are those containing CH in the TLS 1.3 column.