# **Vendor FRTC Questionnaire**

1. What smart card readers does the solution support for the *time of registration*?
2. What biometric readers does the solution support for the *time of registration*?
3. Does the product utilize Microsoft Windows CAPI or an alternative?
4. Does it use the ***Local Machine*** Certificate Store or the ***Current User*** Certificate Store if it uses Microsoft CAPI?
5. If Microsoft CAPI is not used, where are the certificates installed for use in the product for FRTC?
6. Where are the OIDs registered or changed within the product?
7. Where are the logs that show the *time of registration* outcome?
8. Where are the logs that show the *time of access* outcome?
9. How do you turn off certificate validation for the *time of registration*?
10. How do you turn off certificate validation for the duration of the *time of access*?
11. Does your solution rely on a validation process within the PACS software to update the user status during access test cases, ensuring they respond as expected?
12. What is the process for verifying the equipment table, specifically the software (SW) and firmware (FW) versions?
13. How to change authentication modes on the reader(s) (PKI-CAK, PKI-AUTH, PKI-CAK+BIO, PKI-AUTH+BIO)?
14. How can the negotiated bit rate on the contact reader be changed to 446 KBps? *(FRTC Test Case 5.18.01)*
15. How can the negotiated bit rate on the contactless reader be changed to 848 KBps? *(FRTC Test Case 5.18.02)*
16. How do you configure the software application to support the use of 128-bit FASC-N for Time of Registration and Time of Access?
17. How do you configure the software application to support the use of a 128-bit UUID for Time of Registration and Time of Access?
18. How do I determine what the PACS system uses as the primary identifier?
19. Does the solution support the multifactor dynamic assignment of an individual reader authentication mode on a time-based schedule? *(FRTC Test Cases 7.07.05 & 7.07.06)* If yes, how is it configured?
20. For new contact PACS readers, the vendor shall provide a test data report documenting conformance for review and approval of contact readers, which shall support ISO/IEC 7816 *(FRTC Test Case 7.07.09)*
21. For new contactless PACS readers, the vendor shall provide a test data report documenting conformance for review, and approval of contactless readers shall support ISO/IEC 14443 Type A *(FRTC Test Case 7.07.10)*
22. The vendor shall confirm the item doing the crypto at the Time of Access (Reader or Controller) and provide the CMVP certificate number for the item as required in the *FRTC test case 7.09.05*.
23. Does the solution leverage a cached copy of the public key extracted at the *time of registration* for signature verification at the *time of access*? (5.02.06)
24. Does the solution support SM-Auth?
25. Does the solution support OCC-Auth?
26. How do you enable fingerprint verification for enrollment or registration?
27. How do you turn off fingerprint verification for enrollment or registration?
28. What objects/values are read from the PIV Card at enrollment?