Addendum # 1 – Questions and Answers

City of Kirkland Request for Proposal – Job # 28-22-IT

Multi-factor Authentication Solution and Professional Services for Implementation

Questions and Answers

1. What type of scan ID card is the city currently using? (Smart RFID Card, HID Card, Mag Strip, etc.)

   Answer: HID Card

2. Is the city open to being issued a second ID card or FOB for more secure authentication?

   Answer: FOB yes, ID card no

3. How does the city ID card authenticate against? Is it tied to Active Directory or something else?

   Answer: Currently it does not get authenticated against anything and is not tied to Active Directory.

4. Is the City of Kirkland interested in a certificate based solution PKI?

   Answer: No.

5. How many hardware tokens are required? (i.e. 10 for the technicians administering the MFA solution or 800 tokens for all users?

   Answer: Yes ~800 for general authentication and ~10 for Technicians

6. What token types are desired vs required? (i.e. Yubikey, smart card, Feitian TOTP)

   Answer: Yubikey, SmartCard (not RFID), TOTP or Mobile App are all acceptable solutions

7. Will you consider a solution that uses standard mobile phones for the MFA authenticator (to prevent the need of purchasing any special hardware tokens, which are easily lost or can be stolen)?

   Answer: If mobile app based, yes. No SMS authentication.

8. Will you consider a solution that uses centrally managed biometrics (face, palm, voice) captured using standard mobile phones?

   Answer: Fingerprint and face are acceptable. Voice, no.

9. Will you consider a solution that uses fingerprint, face, and iris biometrics that are captured and verified on standard mobile phones?

   Answer: Fingerprint and face, yes. Iris no, people still have concerns about scanning eyes.

10. Does the City want to go passwordless and save time and money?

    Answer: No. We are most interested in the combination to get something you know and something you have.

11. Does the City use Active Directory on-premises for some or all of your user store and authentication?

    Answer: Yes

12. Are you using Azure Active Directory for some or all of your user store and authentication?

    Answer: Yes

13. Are you using Azure Active Directory External Identities for some of your users?

    Answer: Yes

14. Are you using Azure Active Directory Premium 1?

    Answer: Yes

15. Are you using Azure Active Directory Premium 2?

    Answer: No

16. Does the City use Azure Active Directory Conditional Access?

    Answer: No

17. Are you using Azure Active Directory B2C?

    Answer: No

18. Compatibility with network equipment - Cisco, Palo Alto - **Can we get more details on the specific kinds of equipment here? Is the expectation that users logging into this equipment (firewalls, routers, etc) will be challenged with MFA?**

    Answer: Palo Alto Firewalls, CISCO ASA and CISCO Network (switches, routers and firewalls). Yes, we would like users logging into this equipment to be challenged with MFA. Expectation here is two-fold. 1.) Auth for users accessing the VPN 2.) Technicians/Engineer managing the equipment (HTTPS/SSH)

19. Compatibility with Tyler - others? - **Based on research, Tyler Technology offers their Public Sector Software as a cloud/SaaS offering. Can we find out if this product offers SAML or some other auth integration?**

    Answer: Currently, Tyler Technologies is the only internal application (has a web interface that is scheduled for utilizing MFA in the near future). In some cases, Tyler is offering MFA via OKTA (for our on-premise applications).

20. MFA options - Hardware - e.g., scan City ID card - **Can we get more details on the scan city ID card? What is the specific manufacturer and card tech specs? Specifically what technology is it and what are the expected use cases with the scan card? How does it work today? Do desktops and systems already have card readers built in to support this?**

    Answer: HID cards are in limited use for some specific application needs. However, not internally managed by the City at this time. Card readers were added on in the form of a small form USB reader. Currently used only in public safety and we do not have to ability to add-on or tack-on to this solution. This could be further explored if the successful bidder is presenting this as a technology.

21. The proposed solution be able to provide multifactor authentication for VPNs, Firewall, Network Switch's, Router, Wireless controllers and web proxy - **This may be similar to question #1** *[now question #18]* **above, but can we get more details and specifics on the actual hardware or VPNs that are being used?**

    Answer: Please see question #18

22. **Is there a desire for a traditional MFA solution (username/password + 2nd factor) and/or Password-less MFA?**

    Answer: Password-less is not really a desire at this time.

23. Will the City provide some Hardware MFA options they plan to use? What systems / devices are currently being used, if any? "Hardware - e.g., scan City ID card"?

    Answer: See #6 and #20

24. Will you expand on this requirement: The bidder should provide SSL certificate wherever required.

    Answer: If the solution chosen is SaaS and requires an SSL certificate for encryption, it would be be the provider's responsibility to provide the certificate and renew it as required.

25. Line 45 in the excel document: Client agent should have anti tamper password. (requires additional credential to uninstall). Do you have an endpoint privilege management solution currently?

    Answer: No

26. What is your MDR solution, and does it digest syslog? Integration with MDR solution to analyze and parse security events/logs generated.

    Answer: The MFA solution would not integrate with the City's MDR solution but should have the ability to forward logs (preferably via syslog)

27. Is this RFP for MFA a requirement of cyber insurance? If so, can you share the insurance company?

    Answer: Our cyber insurance is a driving factor for this project, but not the only one. The City prefers not to share the name of our insurance company at this time.

28. Will you list the MFA use cases? For example, MFA for VPN, O365, Windows server login and RDP.

    Answer: MFA for VPN, O365, Windows server login, RDP and SaaS applications that utilize SSO.

29. The City notes 30 IT department staff and 800 end users, is the total user count for a license 830? Will the City breakdown provide an end user breakdown of the total user count (e.g., employees, citizens, vendors, etc.)?

    Answer: The 30 IT department staff are included in the 800 end users. Non-employees will be a small set, probably less than 25.

30. What is Tyler and others? Are these applications with a web interface? Line 5 of excel document.

    Answer: See #19

31. Can you describe the expected behavior or requirement for lines 14 and 15 of the excel document: Smart phones – Apple, Android, other? Tablets – Apple, Android, other?

    Answer: The assumption is, if an APP based solution is chosen, it would be compatible and work with all of these technologies. If the solution is hardware based (fob, USB key, card, etc.) there would need to be compatible or alternative ways of authenticating staff on these devices.

32. For line 18 of the excel document, will you clarify "login malfunction" scenario. "Provide strong emergency login mechanism during solution malfunction."

    Answer: We are looking for login options in the event the MFA solution malfunctions or fails.

33. Our standard practice is to assign specific team members further in the sales process, like upon award. Are you open to general descriptions and experience of our implementation team and roles? Or would you understand the people may change according to contract and project start dates, if resumes are included in the response?

    Answer: We prefer seeing information on the people that would be doing the actual work, but

understand that it not always possible.

34. Our company policy is to submit our SOC 2 under a signed NDA. Is it acceptable to either establish the NDA before the submission due date, or provide the SOC 2 later once an NDA is in place?

    Answer: NDAs and SOC 2 reports would happen at contract signing utilizing the documents that were attached to the RFP.

35. How do you manage identities for citizen users?

    Answer: We do not have a category for citizen user accounts on our internal network.

36. Do you require MFA integration with your PAM solution?

    Answer: We have a Privileged Account Management solution that we are interested in integrating with MFA