Organization for Security and Co-operation in Europe

Date: 6 August 2019

Clarification Note No. 1
Invitation to Bid - ITB/SEC/21/2019
Provision of “Multi-factor Authentication Services” and Related Services for the OSCE

The Organization for Security and Co-operation in Europe has received request for clarifications from potential bidders. In accordance with Article 17 of the ITB document, the OSCE would like to provide the following clarification:

Question 1: What is your definition of a MFA server? Does it mean the management system for the certificate issuing?

Answer 1: Yes, it is the management server.

Question 2: What is the use case for using RFID with certificates?

Answer 2: In addition to physically inserting the smartcard into a reading device, we would like to have the option to use it contactless as well.

Question 3: What is meant by “Backend support: Windows Server 2016, Active Directory functional level 2016, vSphere 6.0, 6.5, 6.7” (point 11): Should the solution be installed on Windows Server 2019 running on VMware? Is Active Directory for a connected user store required?

Answer 3: The MFA solution including server, client and all other required components need to support the versions of Windows Server and Active Directory as requested. Furthermore, it needs to be supported to run on the requested vSphere platforms.
The solution should be installed on Windows Server 2016. AD should be used as the user store/source.

Question 4: 5.1.11.) Backend Support - Can you please elaborate on this requirement - beside Active Directory, what type of Backend support is required from Windows Server 2016 and vSphere 6.0, 6.5, 6.7?

Answer 4: The solution must be supported for these product versions by the bidder/vendor

Question 5: **Requirement 11: Backend support: vSphere 6.0, 6.5, 6.7**
Could you please specify if this is a requirement to be able to deploy MFA server(s) as VMWare virtual machine(s) or is the requirement to support MFA logon to vCenter (part of vSphere)?

Answer 5: To deploy it on a VM.

Question 6: What exactly is meant by “Frontend support: Windows 10 Enterprise. (new versions of Windows 10 must be supported within 3 month of the release) (point 12): does this refer to the systems on which smart cards are used or to computers which are used for management?

Answer 6: The MFA client or components (including smartcard readers) need to be supported on Windows 10 Enterprise. Microsoft is releasing new versions of Windows 10 twice a year. The solution should be supported 3 months after the release of the new version.

Question 7: **Requirement 12: Frontend support: Windows 10 Enterprise (new versions/releases of Windows 10 must be supported within 3 month of the release), CentOS 7.3 and above.**
- a) Support for CentOS is mentioned in point 12 in section 5.1, however it no longer appears in the requirements table – is support for CentOS required?

b) If yes, is it required to support smartcard logon at the CentOS desktop (with the PKI device connected directly to the CentOS desktop PC), or via SSH client launched on Windows client? In the first case is required could you please provide number of CentOS workstations to be protected?

Answer 7:

a) This is a mistake from our side and it should be in the optional part.

b) Up to 10 workstation, directly on the desktop. If SSH authentication is possible, then please mention this as well.

Question 8: Point 31 asks for mobile apps. It is not clear for the bidder for which scenario a mobile app would be needed? The solution which the bidder has chosen does not provide mobile apps.

Answer 8: The MFA solution should be offering authentication via iOS or Android apps. Please note that we seek a solution that is offering all required methods. However, in case the solution offered does not provide one or more please mention this in the bid.

Question 9: 5.1.2.) Support for Microsoft PKI - Can you please elaborate on this requirement. (Being able to authenticate users or devices with certificates issued by Windows CA?)

Answer 9: The solution must be able to utilize the Microsoft CA for issuing, revoking and all other tasks that are part of the lifecycle.

Question 10: 5.1.3.) Offline Authentication - Can you please elaborate on this requirement.

Answer 10: It must be possible to authenticate without connection to the MFA server or AD (if user accounts are already cached)

Question 11: 5.1.5.) RDP Multihop / pass-through aware - Can you please elaborate on this requirement - what does it mean to be aware?

Answer 11: This means that when you RDP from computer A to computer B and then from computer B to computer C and then from computer C to computer D, the solution must be able to manage the authentication via smartcard and apply policies etc.

Question 12: 5.1.15.) Role Based Access Control for MFA roles - Please elaborate

Answer 12: The MFA solution must offer different roles for access rights (security) and task assignments (functions).

Question 13: 5.1.20.) Support for and Integration with external services - please elaborate on what services and authentication methods are required.

Answer 13: Office 365 for example with smartcards

Question 14: 5.1.23.) Auditing capabilities - please elaborate

Answer 14: Auditing on enrollments, logins, changes in the MFA system.

Question 15: 5.1.26.) Support for strong authentication to the MFA Management System (no passwords) - please elaborate on what type of authentication is required?

Answer 15: Possibility to authenticate to the MFA system itself for management with smartcards.

Question 16: 5.2) Bidder must offer the following types of devices/authentication methods): Mobile/software authentication (via iOS or Android app) - please elborate on this requirement - does mobile token app falls within this requirement

Answer 16: If it fulfills the requirements, yes

Question 17: 5.1 - #6 - What are the requirements towards a self-service portal?
What functionality is required – a SmartCard request? A temporary revocation of a SmartCard? A Certificate request?

Answer 17: Lifecycle of the smartcard like initialization, PIN operations, certificate issuing, etc.

Question 18: #12 - For Centos support, is it required to authenticate to Centos through SSH or directly on workstation desktop. Please provide more details on this requirement.

Answer 18: Directly on desktop is a must, SSH would be desirable as well

Question 19: Requirement 12: Frontend support: Windows 10 Enterprise (new versions/releases of Windows 10 must be supported within 3 month of the release), CentOS 7.3 and above.
- a) Support for CentOS is mentioned in point 12 in section 5.1, however it no longer appears in the requirements table – is support for CentOS required?

b) If yes, is it required to support smartcard logon at the CentOS desktop (with the PKI device connected directly to the CentOS desktop PC), or via SSH client launched on Windows client? In the first case is required could you please provide number of CentOS workstations to be protected?

Answer 19: **a)** This is a mistake from our side and it should be in the optional part.
b) Up to 10 workstation, directly on the desktop. If SSH authentication is possible, then please mention this as well.

Question 20: Re**:** 18 - What exactly do you mean by Emergency/ rescue token support. Please provide more details. Are we speaking about a SmartCard here?

Answer 20: It should be a way for the MFA admin to allow the user to login to systems in emergency cases like smartcard not working, etc.

Question 21: Re: 22 - What kind of reports are required? What data do you want to analyze?

Answer 21: Login details, system changes

Question 22: How is the user account being created? Frist in ActiveDirectory and the provisioned to the MFA solution or the other way round?
- What kind of resources is authentication required besides Office365? How about Windows Domain, VPN or any other ?

Answer 22: The account will be always created in AD first. Other systems include CheckPoint VPN, webapplications and others.

Question 23: Re**:** licenses: How many MFA licenses will be deployed? For all 4.000 OSCE employees?

Answer 23: Initially, it will be for ICT administrators only (~ 150 to 200)

Question 24: Re: support: What if something unexpected happens outside the support hours? Do you wait until next working day or do you need some emergency number?

Answer 24: 9x5 is a must, everything in addition can be offered as optional.

Question 25: Re: 3. Scope of Services: Is it possible to have remote access to the on premise MFA server to provide the MFA managed services as described in Point 3?

Answer 25: Yes, but only via VPN

Question 26: Re: 5.1. Functional Requirements Point 14: Do you mean the backup of the configuration/database of the MFA solution or do you mean a complete backup of the MFA application including the MFA application, certificates, recovery keys and the device registrations?

Answer 26: This depends a lot on the solution but in general everything that is needed to recover the solution needs to be backed up. Other items may be excluded. Example: As user certificates are issued by the MS CA, I do not expect that these will be backed up.

Question 27: 5.1. Functional requirements Point 4: Only one appliance or software deployed solution should handle the multi forest/domain MFA capabilities or it is fine to have multiple MFA servers to handle the other forest or domain requests? If yes on how many sites/branches a MFA server would be installed?

Answer 27: Preferably one, but in case more will be needed we will have one central location where both MFA servers will be installed. Please note that certificates of both Domains need to be stored on one smartcard.

Question 28: 5.2 Functional Requirements: Do the devices have to support both RFID and NFC or just one of these techniques?

Answer 28: At least one.

Question 29: Re: 9. Multiple certificates from different user accounts can be saved on a single device. **-** Would you be able to specify how many keys/certificates from different user accounts are going to be stored on a single PKI device?

Answer 29: Minimum 6 are required

Question 30: Re: 9. Multiple certificates from different user accounts can be saved on a single device. **-** How many users are going to have such smartcards containing certificates from different user accounts?

Answer 30: Almost all

Question 31: Re: 28: Bidder must offer the following types of devices/ authentication methods): Smartcards.
Should smartcards be equipped with the contactless RFID antenna for door/gate access? If yes, what RFID technology is planned to be used?

Answer 31: It is not foreseen to use it as door/gate access cards at the moment.

Question 32: Re: 31: Bidder must offer the following types of devices/authentication methods): Mobile/software authentication (via iOS or Android app).
- Could you please specify how many users are going to use mobile devices for authentication?

Answer 32: This might be planned for a later stage, but it is important for us that the solution offers the possibility.

Note: Bids must be received no later than **22 August 2019 at 12:00 hr. (CEST)**.
Bids received after the designated time will be automatically rejected.
Submission of bids by fax or email is not accepted.