Organization for Security and Co-operation in Europe

Date: 20 August 2018

Clarification Note No. 2

Invitation to Bid - ITB/SEC/17/2018

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: Point 30 of the Mandatory Requirements (Point 5.2 of the ToR) asks for combined devices. Unfortunately, combined devices are non-standard and can normally only be offered as a special built for individual customer specifications and for large quantities. We would therefore ask to convert this requirement to an optional requirement or only ask for standard devices.

Answer 1: The requirement will be converted to an optional requirement. However, please provide detailed information on quantities required and functionality.

Question 2: 3. Scope of Services - MFA support services: Annual managed service.
5.1. Functional requirements - 2. Support for Microsoft PKI CA

There's no pricing or any further reference for an annual managed service. Could you please clarify this requirement?

Answer 2: This refers to consultancy hours/pool hours.

Question 3: Could please elaborate the supported requirements for Microsoft PKI?

Answer 3: Certificates from Microsoft PKI CAs shall be requested and used on the authentication devices.

Question 4: 5.1. Functional requirements - 3. Offline Authentication
Can you please clarify the offline authentication requirements? E.g. authentication to function without signal/connectivity between authenticator and service as in a self-contained device?

Answer 4: This refers to authentication with certificates on Smartcards or other physical authentication devices.
Authentication has to work without connection to the MFA backend infrastructure, as Active Directory is the authenticator.

Question 5: 5.1. Functional requirements - 5 RDP multi-hop aware
(device connected to computer A, RDP session from computer A to computer B, another RDP session with the device connected to computer A from computer B to computer C etc.)

What RDP version/setup are you using? Is there a Broker or Gateway involved and can you describe the architecture? Are these gateways able to pass-through the authentication method?

Answer 5: RDP of various Windows versions (Win10, Server 2016).
Brokers or Gateways are not planned initially.

The architecture is very simple: Admin connects from client to server, from this server to another server and to another server.
Servers might be terminal/RDS servers or simple member servers.

Please refer to the Microsoft documentation for standard Windows RDP pass-through functionality.

Question 6: 5.1. Functional requirements - 6. Device should only be usable on the device it is physically connected to (this means that when an RDP session will be established to a computer that has a device connected to, it will not be available for use). This seems to contradict with 5.1.3.
How should this be handled if device ports are managed/blocked?

Answer 6: Good scenario:
Device is connected to computer A, which is the physical device that is used by the administrator.
RDP session from computer A will be established to computer B.
From computer B, an RDP session will be established to computer C using the authentication device connected to computer A.

Bad scenario:
Device is connected to computer B. RDP session from computer A will be established to computer B.
From computer B, an RDP session will be established to computer C using the authentication device connected to computer B.

The device should ONLY be available for use if connected to the physical computer where the INITIAL RDP session will be established.

Question 7: 5.1. Functional requirements - 13. Frontend support: Windows 10 Enterprise. What exact Windows 10 version is being used? Are other os version also part of the scope (, MacOs, Linux, Windows 7, 2000, etc.)?

Answer 7: Windows 10 Enterprise 1803.
Future versions like 1809 or 1903 should be supported maximum within 1-2 months after public release.

Question 8: 5.1. Functional requirements - 18. MFA server on premise.
As an optional requirement the MFA Server can be hosted in the cloud. For certain functionalities, e.g. Push Notifications cloud services are compulsory, would this be an accepted scenario?

Answer 8: On premise installation of the MFA server is a mandatory requirement.

Question 9: 5.1. Functional requirements - 21. Automated revocation of certificates on the CA once removed from the MFA system (lifecycle management).

This should be the functionality of the PKI and not the MFA service.
Please clarify the desired functionality further?

Answer 9: It's a feature of the CA BUT the MFA solution needs an interface/API to the CA to automatically perform/request such an action.

Question 10: 5.2. Device requirements - Bidder must offer the following types of devices/authentication methods):

- Smartcards.
- USB eTokens.
- OTP (One-Time Passwords).
- RFID/NFC/Bluetooth.
- Combined devices.
- Mobile/software authentication (via iOS or Android app).

USB eTokens is a specific vendor type. Can other Tokens be offered? What if one of the methods cannot be offered, are other methods, e.g. SMS/Voice, risk-analytics, FIDO U2F compliant tokens, valid?

Answer 10: Alternative physical authentication devices to eTokens with the same functionality will be accepted. However, they need to support the requested connectivity methods like USB.

The devices/methods listed are mandatory.
However, other methods can be offered in addition.

Question 11: 5.2. Device requirements

Devices must not have an expiration date.
Devices must be available in 2 colours or more.

Can you please clarify the expiration date and colouring requirements?
Are customer specific labels a valid option?

Answer 11: Devices should be usable indefinitely and should not expire after a number of years.
Colouring would be the preferred option.
However, customer specific labels might be acceptable.
Please add a picture/example of the customer specific label to the offer.

Question 12: 5.4 Optional Requirements - Information/notification to users that certificate will expire soon.
This should be the functionality of the PKI and not the MFA service.
Please clarify the desired functionality further?

Answer 12: We expect that this functionality will be provided by the MFA solution
In case you offer a different solution, please describe how this will be done (e.g. detailed architecture and configuration of the PKI).

Question 13: 5.4 Optional Requirements -
Possibility to use 3rd party certificates from a managed enterprise PKI (e.g. DigiCert, GlobalSign etc.).

Can you clarify how these 3rd party certificates should be used?

Answer 13: The same way as the Microsoft PKI CA issued certificates.