– Unsupported OS - The list of supported operating systems contains Windows 2008 R2 and 2012 which are out of support from Microsoft. Do you require this Windows versions as a "must be required/supported"?

- Windows 2008 R2 and Windows 2012 should be supported by the vendor (best effort).

– What type of OS have desktops and laptops installed? Is it Windows OS only? Is Linux OS used only on servers?

- Windows only (Windows 10). Linux OS is used on servers only.

– HTTPS inspection - Do you use some service with SSL inspection in your curent setup? It is possible to use it in this project? Or should it be in scope of the tender? Do you prefer cloud-based solution or on-premise?

- We're looking for a product/solution that will perform HTTPS inspection on the client side, to avoid using centralized proxying.

– Virtual servers (1100) - Are the servers for application (application servers) or do you have any RDP/VDI servers?

- A mix of both (application servers being a majority). There are no VDIs, but RDSH services.

– Microsoft 365 environment
Do you have single or multiple M365 tenants?

- Single.

– What type of M365 licenses do you have?

- E3

– Do you accept only swiss location-based cloud environments or also for example like Germany West Central or EU based?

- We are going to accept Germany West Central and EU based proposals too.

– There is no Price Proposal Template in the tender documentation. Will you provide one, or is it up to us to create it? Please give us at least a clue. Lump sum? Per profile? Annually?

- It's up to you to provide the pricing proposal. If there is price difference between profiles, then annual costs per profile would be sufficient, otherwise, cumulative annual price is enough.

– Are they technical criteria in chapter 4 which are eliminatory when not available in the solution ?

- The mandatory components are:

– Physical assets: Threat prevention and threat hunting, access control, web protection, data protection, MDR

- Virtual assets: Threat prevention and threat hunting, web protection, MDR

– Is Digigal signature allowed to sign the documents, or do we need to print out sign manually and scan the signed document ?

- Yes

– What are the operating systems in use on the different assets (physical and virtual)? How many Linux devices and how many Windows devies?

- All physical assets are powered by Windows 10, virtual assets are powered by Windows Servers (2008 R2, 2012, 2012 R2, 2016, 2019, 2022). The number of Linux devices is neglectable (less than 1% of all virtual assets).

– Could the solution rely on other mechanisms similar and as effective as the Intel vPro(R) platform's Threat Detection Technology (TDT)?

- Yes.

- Do you require URL Filtering and Web traffic protection (4.1.5) to be handled on the endpoint?
  - Yes, since we'd like to avoid using centralized proxying.

- Does the Host Isolation have to be automated directly via the endpoint security management server or could it be handled by an MDR/SOAR or SIEM solution ?
  - The host isolation event could be handled either by the endpoint or MDR/SOAR solution.

- How many users need VPN remote access? In average how many concurrent VPN connections are expected ?
  - 350 / 350

- Chapter 3.7, how de we need to understand the sentence with the Monthly payement. Is this specific for the services proposed by the bidder for the installation and provisioning. The Licenses and Vendors item will be payed upfront for the durantion of the contract.
  - This has been taken from the standard template and might have been overlooked/not be applicable. The important part is: The delivery and payment schedules should be proposed by Bidders in their pricing structures, and must be agreed with the UPU. Please propose your payment schedule in your offer. We assume that it might be done on a yearly basis.

- Is the MDR solution intended for only the endpoints or will be covering other assets like the Firewalls?
  - If there are additional costs involved by covering other assets (without possibility of agent to be installed), please specify so.

- Preferred duration for the log retention (3 months, 1 year)
  - Minimum 3 months.

- Do you require the same editor to provide both the Endpoint Security and the MDR service?
  - I assume you mean vendor by editor? We're looking for a vendor that can combine both services into one solution. We will consider multi solution proposals as long as we are contractually engaged with one vendor.

- Is Threat emulation/extration required on the servers?
  - Yes.

- Are performance Data for Firewalls known or defined? Throuput/Sessions p. second, Inteface Speeds/Form Factor, Redundancy, number of reqired Virtual Firewalls in the appliance

  - The firewall functionality should be implemented on the endpoints' side (laptop/PC) and be part of the endpoint suite.
- Is Firewall Redundancy subject to specific requirements? Distributed Clustering, Active-Active/Passive setup
  - We're looking for the firewall functionality on endpoints.

Question ID	Chapters		Description	Question
1	2,4	Background	combining all functionalities in a unique solution	Is it a must to provide all functionalities in a unique solution ? What do you mean by solution, is it a unique agent or unique vendor ? **By unique we assume a solution that will allow us to manage all aspects of endpoint protection via one console or management portal. We also assume that there will be only one agent installed.**
2	4,1,4	Access Control	Remote Access VPN	Can we propose a replacement of your VPN Gateway and your Internet Proxy by a new Firewall Cluster ? **Yes, for the VPN gateway.** **As for the Internet Proxy: we are looking for a solution that will perform web filtering and SSL inspection on the client/endpoint side, to avoid routing of web traffic to some proxy or gateway.**
3	4,1,4	Access Control	Firewall	What is your current Internet Firewall Model ? What is the current Internet throughput ? How many DMZ do you have ? **It's a classical North-South setup with several DMZs. The Internet bandwidth is 1Gbps.** **Please note that the firewall functionality requested in this RFP is related to the ability to deploy and manage firewall rules on all managed endpoints (specifically on physical assets such as laptops). The overall firewall setup is not part of this RFP.**

Question ID	Chapters		Description	Question
4	4,1,4	Access Control	Firewall	Do you already perform the SSL decription ? **Yes, we currently route all web traffic to the SSL inspection gateways.** **We are looking for a solution that will perform web filtering and SSL inspection on the client/endpoint side.**
5	4,1,4	Access Control	Firewall	Do you have some specific FW interface requirement ? **Please note that the firewall functionality requested in this RFP is related to the ability to deploy and manage firewall rules on all managed endpoints (specifically on physical assets such as laptops). The overall firewall setup is not part of this RFP.**

ID#	Questions Hacknowledge	Answers
#01	Is there any other document to consider in your RFP beside the Call for tender pdf file (https://www.upu.int/UPU/media/upu/TPC_CAA/RFPs/2020/RFP-2023-025-DCTP-Endpoint-Protection.pdf)?	No
#02	Could you provide the UPU General Terms and Conditions (*§3.8*)?	https://www.upu.int/en/Universal-Postal-Union/Procurement#reference-documents
#03	*4.1.8 Managed detection and response (MDR); Monitoring of security events ; 24×7×365 monitoring of security events* Could you confirm that you request a 24x7x365 for the Response as well?	Confirmed
#04	Do you already use a SOC solution (Security Operations Center)?	Yes
#05	Do you already use a SIEM solution (Security Information and Event Management)? If yes, on what kind of technology?	No
#06	If not already use, would you be ok to activate Microsoft Sentinel as a SIEM to managed the alerts?	Yes
#07	Do you already have a Microsoft subscription (f.ex. E3 or E5)?	Yes (E3)
#08	If no, do you already have subscribed for MDE – Microsoft Defender for Endpoint, or do you want the provider to integrate the EDR licences' costs in his quote?	Not sure we've subscribed, to be checked
#09	What are the response time (SLA) for reporting (Detection) and handling (Response) for the alerts required to the provider? Could we provide different SLA between business-hours and outside-business-hours shifts?	Yes, different SLAs would help
#10	Would you be interested, in option, to monitor the network activities with an IDS ? If yes how many sites (DataCenter, Buildings, Remote sites…) are to consider?	Yes. There are three DCs, all located in Bern.
#11	*4.1.4 Access control (applicable for physical assets) - Remote access VPN*: Do you have a VPN already installed (and your requirement is related to the security monitoring of the solution) or do you require support for the VPN deployment / management?	We currently use a mix of different brands and technologies (SSL VPN and IPsec) and we expect your solution to unify and package the VPN solution. There are no any requirements for the integration nor inheritance with our existing technologies, so please propose your solution.
#12	*4.1.6. Data protection - Full disk encryption*: Do you require the provider to implement, deploy and manage the device encryption or to support your team with a technology compatible with the EDR?	The proposed solution should implement or manage the device encryption. We also expect from the vendor initial support during setting up templates. The actual deployment will be done by local team.

– Confirm for question #11 that your requirement consists of securing the connectivity between you and us for the service we provide (not managing your existing VPN).
  - **Our requirement is to provide secure access to the internal (on-premise) resources for the stuff travelling or working from home. If your solution requires additional VPN for the management, please indicate so.**

1. Considering the solution components and complexity of the scope and the thoroughness required in our response, we kindly request an extension of the RFP submission deadline till **20th December 2023**. Please confirm?
   - **Considering that UPU will be closed on the 24th of December, we'd like to have some time to analyze received proposals prior to the office closure, therefore, we could extend the deadline for one more week, till 15th of December, 17:00 CET.**

2. With reference to **Section 3.6 Pricing Structure** in the RFP document, you have requested a detailed pricing structure to be included in our response. Do you have any specific **pricing template or format** to be followed? If so, please share with us.
   - **There is no template, please propose the structure that suits you better.**

3. We assume that any licenses associated with this scope will be procured by UPU. Please confirm?
   - **Confirmed, assuming that you will provide us with the clear overview and costs of required licenses.**

#	Chapter	Requirement	Question
1	4.1.3 Sandboxing and threat extraction (applicable for all assets)	Content disarm and reconstruction (CDR) - Extraction and removal of harmful and exploitable content to eliminate potential threats	Does this need to be done on the endpoint and/or at the network perimeter ? **Endpoint.**
2	4.1.3 Sandboxing and threat extraction (applicable for all assets)	Extraction and discovery of threats hidden in SSL/TLS communications	SSL/TLS decryption usually occurs at the network level. Does this need to be implemented at the VPN perimeter only ? or/and at the Internet perimeter ? or/and at the datacenter between endpoint and internal servers ? **We are looking for the solution that can implement SSL inspection at the endpoint level.**
3	4.1.4 – Access Control (applicable for physical Assets)	Firewall rules controlling access to/from endpoints based on IP addresses, domains, ports and protocols	Does this need to be implemented at the network level too ? If yes, does this need to be implemented at the VPN perimeter only ? **The firewall functionality is expected to be implemented on the endpoint level.**
4	4.1.4 – Access Control (applicable for physical Assets)	Guaranteed compliance of endpoints with the UPU's security rules, enabling enforcement of restrictive policies in the event of non-compliance	Does this need to be implemented also for internal (LAN) network connectivity ? **Yes.** What exactly is meant by "compliance of endpoints" ? **For example, prohibiting of VPN connectivity in case of OS updates or antivirus definitions are outdated.** **Or** **Prohibiting of certain traffic in case of a certain (vulnerable) version of software discovered.**

#	Chapter	Requirement	Question
5	4.1.5 – Web protection (applicable for all assets)	URL Filtering, Zero-phishing protection, Corporate credential protection	Does this apply only to remote users connecting through the VPN gateway ? **This applies to all audience, both accessing Internet from on-premise networks and remote users.**
6	2.20	Estimated start of engagement	Is there any flexibility with the estimated start of engagement date of 15 January 2024? **Please clarify what flexibility is required?**

- The solution we propose involves, in addition to the EDR solution, the implementation of a pair of physical appliances (firewall/VPN) to meet the technical requirements outlined in your specifications. Is such a hybrid solution acceptable or disqualifying?
  - **This solution is acceptable. However, we'd like to emphasize that the firewall functionality requested in this RFP is related to the ability to deploy and manage firewall rules on all managed endpoints (specifically on physical assets such as laptops).**

    If VPN connectivity requires additional appliances, please include them in your proposal.

Is it planned that the tender will be responsible for the operation of requirement 4.1.6? **I didn't understand the question. The proposed solution should be capable to perform disk encryption in an automated manner.**
Who is responsible for the Device Management Solution? **Device Management solution is not part of this RFP.**
Which AV/EDR Solutions are now in place? **Not relevant.**
Who will be responsible for deinstalling the current AV/EDR solution? **UPU**
If the tender can demonstrate UPU that point 4.1.3 is not necessary with his EDR solution, can we ignore this requirement? **Yes**
Transparent VPN connectivity should support, environments with the captive portal deployed: Which parts of the network or which applications require Captive Portal? What are the user Groups which would use this function? Can you provide some screenshots? **This is linked to the various captive portals used outside of the UPU premises, such as public cafes or airports.**
URL-Filtering: Can the Function be realised with Client Software on a laptop, which has more functionality than a browser plugin? **Yes**
Is a later start date after 15 Jan 2024 possible? Hardware lead times and Onboarding will require more time to plan **No**

- Does UPU only have one tenant?
  All domains are on premise.
  Question:
  Does this mean there is no Azure AD tenant, and intune tenant?

- ***There is Azure AD tenant, but no integration with endpoints. There is no Intune tenant.***

– **Question:**
What licenses does UPU have in general today?
Please clarify what licenses are you referring to?
  - **We are referring to Azure licenses.**

P1

Question	Answer
Could you kindly verify that the inventory listed below is accurate? 1600 Endpoints 500 desktops, laptops 1100 virtual servers 350 Users	Confirmed
What technology stack are you considering for your Endpoint Protection Project? (e.g. Microsoft Defender?)	We don't have any considerations regarding the stack – the purpose of this RFP is to find one
Could you share information on the Microsoft licenses you have in place for your endpoints, both clients and servers, in relation to endpoint security? It would be helpful to know the quantity of each license as well.	E3 (less than 500)
Have you had the chance to set up Microsoft Sentinel? If not, do you currently have an Azure Tenant?	Sentinel is not setup/configured. We do have Azure Tenant.
Are there any other cloud platforms where you currently have a presence? (e.g. AWS)	No

4.1.5 Corporate Credential Protection	Solution suggested by us implies a Firewall Appliance (HW or VM) to cover certian requirements as Credential Phishing Protection. Would this be a viable option to implement the solution with a Firewall Appliance on the network additinally to the Endpoint Software on Clients? **Yes**
4.1.4 Remote Access VPN	Where to Clients establish a VPN Connecton to on premises? Is there a VPN Gateway in place? **The VPN is established to the on-premise VPN gateway (IPSec and SSL VPN).**
4.1.5 URL Filtering	Should HTTPS inspection be also implemented on the Endpoint itself? **Yes**
4.1.4 Firewall	Is blocking of Ips on the Client Software a must feature or would it suffice to be able to block the Applications, Domains (Application Firewall Functionality)? **The firewall functionality is requested as a protection measure for travelling staff accessing public resources (either via wireless or wired connectivity)**

General	Are you looking for endpoint only based solution to connect to an existing on Prem/DC Infrastructure or are you aiming towards a SASE/SSE Solution? **Both options are applicable and will be considered/evaluated**
General	Can Endpoints be managed over the Cloud or should they be managed on prem? **Both options are applicable and will be considered/evaluated**