JHUBDIGITAL
Ministry of Defence
Ground Floor
Main Building
Whitehall
London SW1A 2HB

MOD Bring Your Own Device (BYOD) Alpha

Background

The Ministry of Defence is modernising the way it works and has a strong desire to provide mobility and flexible ways of working for its entire workforce.

The MOD has a corporate IT system called MODNET, which operates in both fixed and deployed locations, working at a classification of OFFICIAL (with caveats e.g. OFFICIAL Sensitive). It is not practicable or financially viable for the MOD to provide all potential MODNET users with their own endpoint device, especially if they only require limited access.

In addition to its own workforce the MOD works with many partners, companies, contractors and temporary staff who also require secure access to MOD data or services hosted on MODNET. Providing temporary access to MODNET necessitates the need for them to be provided with MODNET accounts, and an associated end user device, often at a direct cost to projects, which is not cost effective or reflective of modern working. Alternatively, information is sent directly to partners, limiting the MOD's control.

Both these scenarios could be addressed by adoption of Bring Your Own Device (BYOD) solutions. For this challenge BYOD will be treated as any endpoint user access device that is not managed as part of the MODNET service. This could include devices owned by an individual, a contractor, a supplier or a MOD device without a MODNET build. Access could be restricted to specific applications, files or anything up to and including all MODNET services. The devices could be trusted or untrusted depending on the scenario, however the user's identity should remain authenticated throughout the session and all information should be protected at the appropriate level.

Wider use of BYOD where it is deemed safe and secure would offer users the opportunity to work more flexibly by providing them with the appropriate access to MOD information and tools, more broadly an increased use of BYOD would lead to:

- Reduction in the number of endpoints procured and supported
- Enable greater access to disadvantaged users
- Improved control of information sharing

Vision

MOD Personas

User personas were identified using the model shown in Fig 1. below. These were used to identify user profiles that would potentially benefit from increased use of BYOD. The diagram provides an indication of the aspects of a persona that will impact on how and where MOD are likely to implement BYOD.

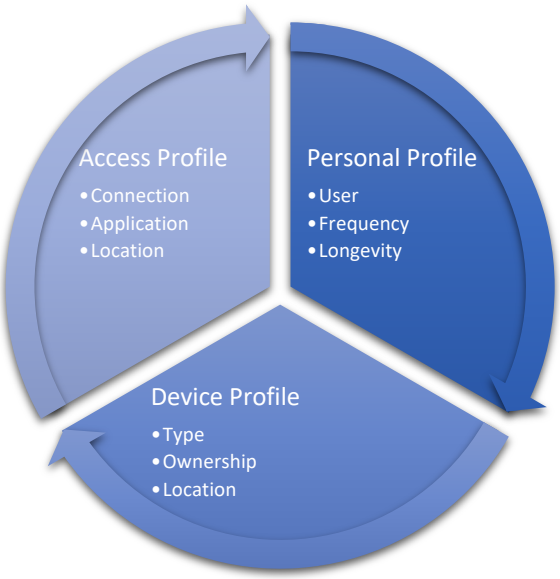

Fig 1.

Six typical user personas were identified where there is the potential to deploy a BYOD solution.

1. **Remote & Restricted (Military or Cadet)**
    - User who currently has limited or no access to MODNET
    - User who does not require all the features on a MODNET account
    - User who requires occasional for specific tasks for example
        - Access to training material whilst not at MOD site
        - Occasional access to secure communications
        - Access to specific services like JPA whilst not at a MOD site e.g. Reservists
2. **Secure On-Call**
    - User waiting to be called in to an incident
    - Secure messaging to personal device to outline the incidents nature
3. **Trusted Supplier / Partner**
    - Requires access to MOD information related to their projects
    - Currently pays for limited MODNET terminals at their premises
    - Alternatively relies on documents being sent by email or CD

- Has an accredited secure network and hardware hosted at a list-x site

4. Consultant

- Bought in for limited time and scope
- Requires access to specific MOD files related to their project
- Currently given full MODNET account, hardware and broad access
- Has their own accredited company hardware

5. Manpower Substitute

- Bought in for limited time to fulfil a MOD role
- Require broad access to MOD files related to their work
- Currently given full MODNET account, hardware and broad access
- Has their own hardware

6. **Detached Duty (Crown Servant)**

- Full time MOD user who spends time away from site
- Requires limited access to services whilst away from MOD site
- Requires access to communication whilst working remotely

More detail of typical access profiles for each of these personas can be found in Annex A.

Issues to Overcome

User Authentication

- How are users identified?
- How is user authentication maintained?

Access Control

- How is access brokered?
- How is access restricted?

Data Security

- How is information protected?
- Where is information stored?
- Can data be retrieved/removed from the device?

Device Management

- How is device status checked on activation?
- How is device status controlled?
- How is device status confirmed during the session?

Network Security

- How is access into the wider network prevented?
- How is access to the network monitored

The Challenge

Are you able to demonstrate solutions that enable BYOD for one or more of the six personas? These solutions should:

- Maintain the security of the network and information
- Work with the current MOD environment (MODNET)
- Be compliant with the current MOD security position or provide evidence to demonstrate why a novel security position would still meets MOD needs
- Be built through the configuration of Common Off The Shelf (COTS) systems
- Be deployable at scale and not cost prohibitive
- Be a mature solution that could be physically demonstrated

The response should address:

- Which persona(s) are being looked at?
- How the issues are being tackled?
- How the solution works?
- A proposal for a demonstration?
- How the solution would work for MOD?

Annex A

Profile	User	Frequency	Longevity	Device	Ownership	Location	Connection	Application
1	Remote & Restricted (Military or Cadet)	Monthly	Permanent	Any	Personal	Home	Insecure	JPA Chat Email
2	Secure On-Call	Incidental	Permanent	Mobile	Personal	Home	Mobile Insecure	Chat
3	Trusted Supplier / Partner	Weekly	Medium Long Term	Desktop Laptop	Company	List-	Secure	Specific SharePoint
4	Consultant	Daily	Short Term	Desktop Laptop	Company	MOD	Secure WIFI	Specific SharePoint
5	Manpower Substitute	Daily	Medium Term	Desktop Laptop	Company Personal	MOD	Secure WIFI	Specific SharePoint O365
6	Detached Duty (Crown Servant)	Daily	Permanent	Mobile	Personal	UK	Mobile Insecure	Email Chat