End User Device Strategy: Interoperability Standards

This document defines the target architecture for cross-government interoperability standards and interfaces between a government End User Device and backend applications, services, platforms. An accompanying document defines the security framework and controls for mobile end user devices to be used for **OFFICIAL** information including **OFFICIAL-SENSITIVE.**

The recommended standards aim to optimise for technology and security assurance, low cost and complexity, minimal 3rd party software, good user experience, wider competition and choice, and improved alignment to the consumer and commodity IT market.

This document examines standards for a mobile laptop with a “thick” operating system installed, such as Linux, Windows or MacOS X. Forthcoming guidance will cover thin client devices, smartphones and tablets but is not expected to vary significantly from the key principles of this guidance.

These standards are currently recommended. Mandated interoperability standards for end user devices will be considered by the Open Standards Board process.

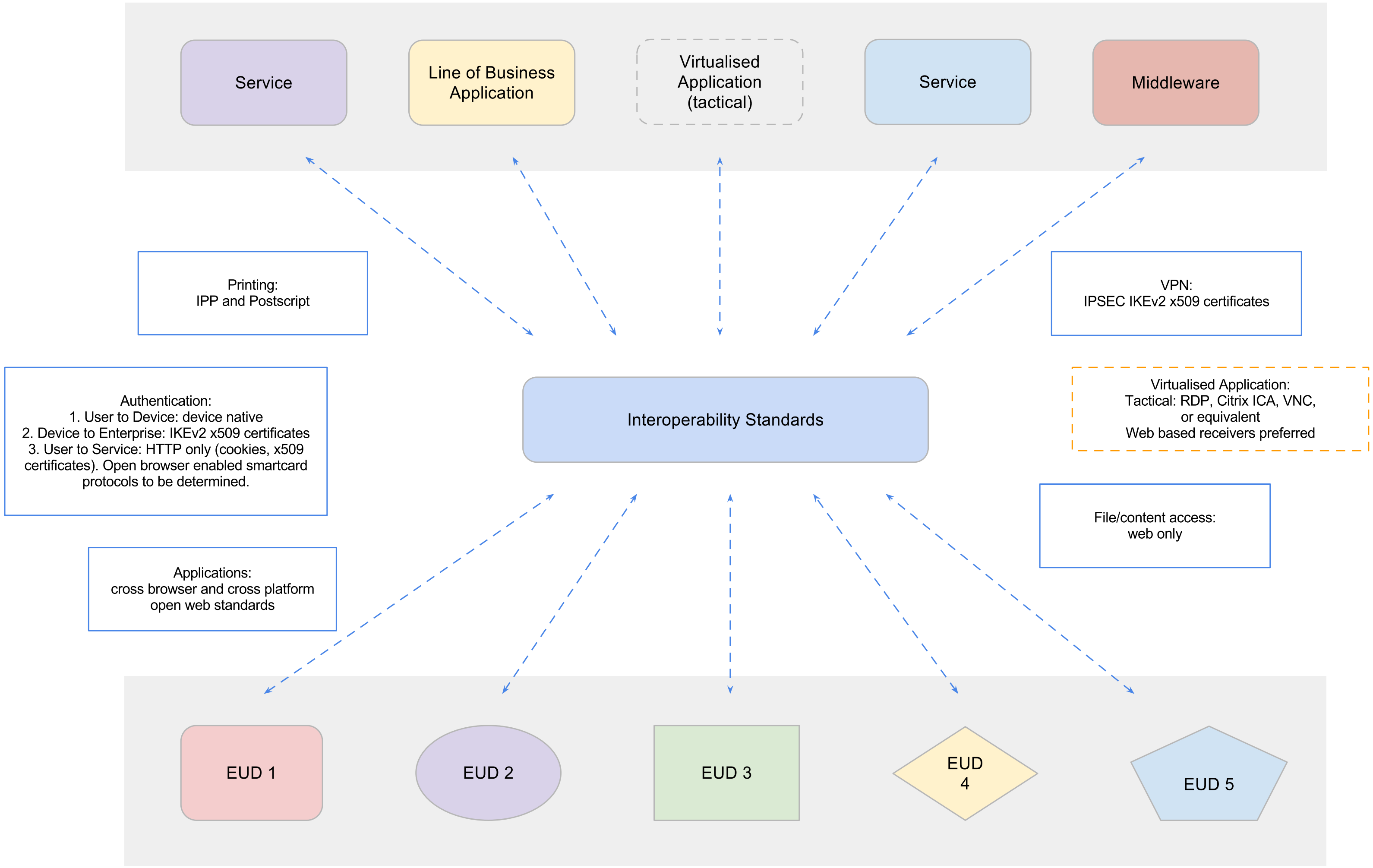
Interoperability

IT Reform strategic goals for interoperability standards are to:

- remove any dependence between backend services or applications, and the end user device or its components (operating system, browser, software), effectively rendering the choice of end user device largely irrelevant
- ensure full interoperability can be achieved using Windows 7 or 8, Linux and Apple Mac OS X devices
- move IT complexity away from end user devices back to platforms and services
- remove bespoke government-only technologies and interactions
- avoid lock-in to particular suppliers or technology products

Interoperability Standards Overview

The following diagram illustrates interoperability standards enabling diverse applications and services to interoperate with different kinds of end user devices, both current and future.



Service
Line of Business Application
Virtualised Application (tactical)
Service
Middleware
Interoperability Standards
EUD 1
EUD 2
EUD 3
EUD 4
EUD 5

Printing:
IPP and Postscript

Authentication:
1. User to Device: device native
2. Device to Enterprise: IKEv2 x509 certificates
3. User to Service: HTTP only (cookies, x509 certificates). Open browser enabled smartcard protocols to be determined.

Applications:
cross browser and cross platform open web standards

VPN:
IPSEC IKEv2 x509 certificates

Virtualised Application:
Tactical: RDP, Citrix ICA, VNC, or equivalent
Web based receivers preferred

File/content access:
web only

Interoperation	Standards	Benefits & Rationale
VPN	**IPsec** using **IKEv2** key exchange. IKEv1 tolerated as interim standard. See security framework document for assurance requirements.	IPsec is an open mature widely implemented standard for VPN, and can be suitably secured. IPsec preferred over TLS/SSL VPNs. Though lighter, open standards for encapsulation of IP traffic over TLS/SSL tunnels are immature making interoperability difficult.
Printing	**Internet Printing Protocol (IPP)** for communicating with queue managers. **Postscript** for print format.	IPP is an open means of communicating with a print server or queue manager, and is supported by the market. Most enterprise class printers also talk IPP. This removes any dependency on any specific vendor. Printers themselves must accept Postscript print jobs. Most enterprise class printers understand Postscript or emulate it successfully. This removes any need for the EUDs to have specific printer drivers installed. Linux and Mac OS X print postscript natively. Windows 7 can have a universal driver installed.

Interoperation	Standards	Benefits & Rationale
Authentication	The approach to user, device and service authentication is as follows: 1. Users authenticate themselves to remote services they require to access (web) 2. Users authenticate themselves to their devices (device native) 3. Devices and the enterprise network mutually authenticate each other (IPsec) All three must be implemented together. See security framework document for assurance requirements.	Using web mechanisms to authenticate ensures services are agnostic to the device and it's operating system. Web based authentication is also becoming the standard for web scale services. Local authentication using the device's native mechanisms is fine as the choice does not impact on other devices or infrastructure. IPsec with IKE provides a suitable mutual authentication mechanism, triggered as part of setting up a VPN connection to the enterprise. It is expected that other software and hardware will make greater use of the machine and user x509 certificates described here.
Authentication: user to service	Authentication to services should be via the **browser** (**HTTP** or **HTTPS**). SSL **X.509** user certificates to authenticate the user to the service, using only the browser mechanisms is also possible once an employee PKI is established. Stronger authentication (eg 2-factor or smartcard authentication) must conform to interoperability standards to be determined. Standards for employee smartcard and hardware tokens will be determined under the Civil Service Reform WorkPlace Transformation stream. Where possible the approach should use the browser as the means of interaction and avoid additional peripherals.	No assumptions about vendor-specific technology. Browser/HTTP based authentication is simple and lightweight. The effect of single sign-on, or shared trust between services, is managed at the back end without any additional imposition on software or capability on the end user device outside of the browser. OFFICIAL-SENSITIVE may require stronger forms of authentication (e.g. smartcard or 2-factor) and may additionally require the user to connect to the service from a particular device.

Interoperation	Standards	Benefits & Rationale
Authentication: user to device	User authenticates to device using its **native** operating system login mechanism. This may be supplemented by a pre-boot authentication step to unlock the encrypted disk. See security framework document for assurance requirements.	Pre boot authentication, where a user provides credentials to unlock an encrypted disk, is often stronger than the native login mechanism.
Authentication: device to enterprise infrastructure	**X.509** machine and gateway certificates which are verified as part of the **IPsec IKEv2** mutual authentication handshake.	The requirement for this authentication is met through the IPsec configuration.
Web	Common cross-browser and **cross-platform web standards**, including HTML5, CSS and Javascript.	Web applications must not require specific browsers, operating systems, plugins or extensions. Java and Flash in-browser runtimes might be tolerated as tactical but their use will be tightly controlled to avoid proliferation and avoid potential legacy and interoperability problems in future.

Interoperation	Standards	Benefits & Rationale
Remote Applications	**Tactical**: remote application viewers. No established mature fully open standard exists which meets expected user experience. Microsoft, Citrix and VMWare, amongst others, offer application virtualisation receivers implemented on a range of operating systems, including Linux and Mac OS X. Where possible, **web based receivers** should be used. Both proprietary and open source web receivers are being developed for viewing remote applications. These include pure-web HTML5 viewers.	Viewing applications remotely is a tactical approach until services transition to pure web only. VNC is an open standard for viewing remote desktops including running applications, with commercial and open source clients to many operating systems. However, VNC does not provide the expected user experience as it is desktop session and not application oriented. Microsoft, Citrix and VMWare, amongst others, offer solutions for virtualising Windows applications and viewing them from a range of operating systems including Linux and Mac OS X. Where possible, native application virtualisation functions should be used, avoiding 3rd party software. Web based clients for viewing applications virtualised by Microsoft, Citrix and VMWare solutions should be preferred over locally installed device specific solutions.
File / Content Access	Web interface only.	The web interface approach is strategically aligned as it minimised complexity at the end user device, and ensures device agnostic services. Where this is not possible, open standards exists for interoperating with file / document content stores. The webDAV protocol is mature and widely implemented.