Cabinet Office

CESG

End User Device Strategy: Security Framework & Controls

This document presents the security framework for End User Devices working with **OFFICIAL** information, and defines the control for mobile laptops to be used for both **OFFICIAL** and **OFFICIAL-SENSITIVE**.

The selected 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 defines 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.

The scope of this document is central government departments, their agencies and related bodies. Wider public sector organisations can use this security framework as part of their broader compliance with the Public Services Network (PSN) codes of connection.

Security

IT Reform strategic goals for a security framework are to:

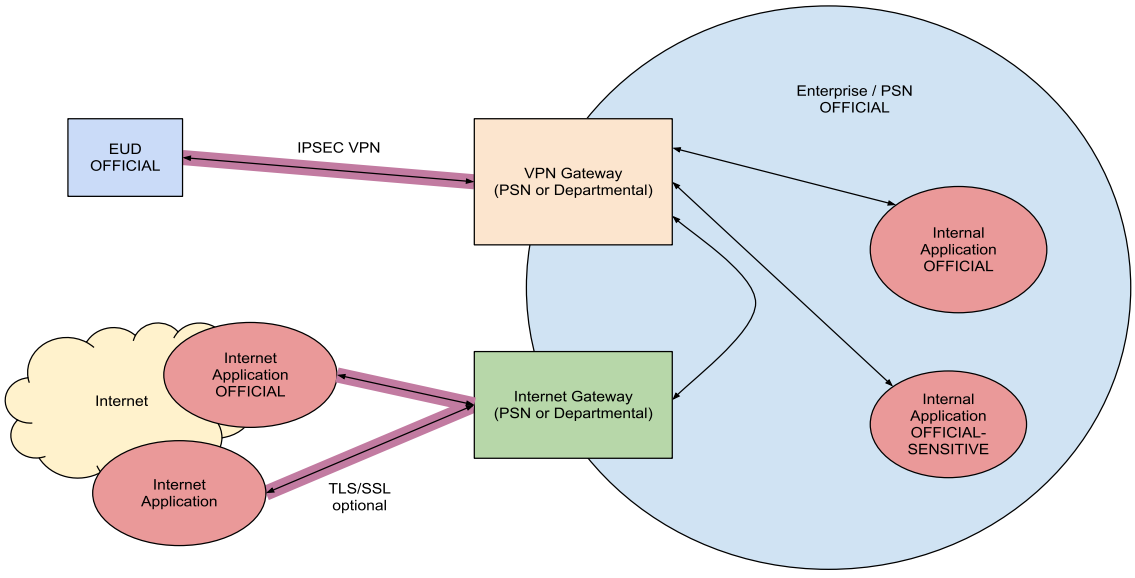
- make optimum use of native security functions, avoiding third party products wherever possible
- make better use of controls around the data and services where they can often be more effective, rather than adding additional complexity to devices
- allow greater user responsibility to reduce security complexity, maintaining user experience for the majority of responsible users
- logging and audit preferred over prevention and control, to maintain user experience and flexibility for the majority of responsible users
- develop a single and sufficient specification for accessing OFFICIAL including OFFICIAL-SENSITIVE, recognising much of the controls will be at the service side
- enable transparency and clarity to widen a correct understanding of the security requirements, widening the market of potential suppliers, and driving down over-specification of security
- enable informed risk management and justification of security controls through traceability between threats, their methods of attack and suggested mitigations
- enable greater interoperability of IT systems through a more common and consistent approach to securing OFFICIAL information

High Level Architecture

The following diagram illustrates the expected high level architecture for end user devices interacting with internal and public services. Key features are:

- Suitably trusted end user device with machine certificate
- No direct access to the internet, only via a corporate internet gateway (no split tunneling)
- Communication between device and enterprise protected by assured IPsec VPN
- Communications to individual web services may be protected by TLS/SSL on a per service requirement. Tunnels broken for inspection, except where personal privacy is necessary, for example personal banking.
- Applications for working with OFFICIAL-SENSITIVE information may challenge user for stronger credentials (employee smartcard, 2-factor) using the standards as defined here and make no further assumptions about device
- Over time the boundaries between departmental perimeters may be less defined as resources and services are shared. However this space will remain within the PSN.

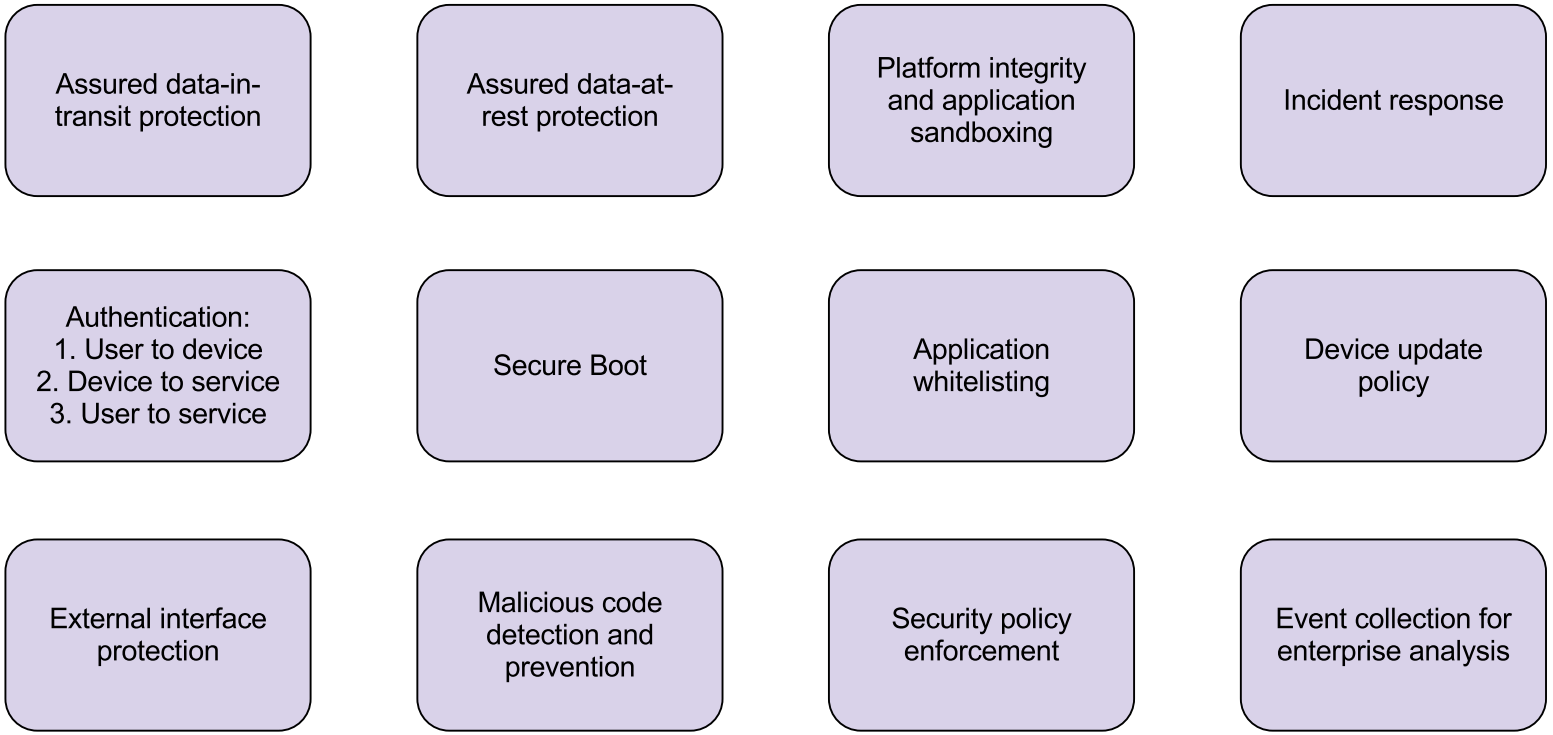
CESG provides detailed guidance for the design and configuration of each of the elements of this high level architecture, for example the Walled Gardens For Remote Access Architectural Pattern.



CESG provides detailed guidance for the design and configuration of each of the elements of this high level architecture, for example the Walled Gardens For Remote Access Architectural Pattern.

Mobile EUD Security Framework for OFFICIAL Information

The following summarises the 12 areas requiring security controls for mobile end user devices working with OFFICIAL information.



Domain	Standards	Benefits & Rationale	Comments & Clarification
Assured data-in-transit protection	**Requirement**: An IPsec client which is assured under the CESG CPA scheme against the *IPsec VPN for Remote Working - Software Client* security characteristic, configured in accordance with the PSN End-State IPsec profile: IKEv2, X.509, AES-128 etc. PSN Interim IPsec profile (acceptable until 2015): IKEv1, X.509, AES-128 etc. http://www.cesg.gov.uk/servicecatalogue/CPA/Pages/Security-Characteristics.aspx	Protecting data as it travels across unprotected bearers between the device and an enterprise network is of critical importance. Independent formal assurance is required due to implementation errors and vulnerabilities often introduced despite vendor assertions to the contrary. PSN profiles were developed in conjunction with the National Technical Authority for Information Assurance's leading cryptographic experts to provide an appropriate level of cryptographic security for the PSN and connected systems and in line with industry good practice. IPsec is a mature set of standards, widely available across many vendors of end user devices and networking equipment.	Native IPsec clients exist for Linux, Mac OS X and Windows 7. Linux and Windows 7 have been demonstrated to function as required. Work is underway to demonstrate the native Mac OS X client functions. CPA assurance of a cross platform open source IPsec client is underway (January 2013). CPA assurance is currently required for the native Mac OS X and Windows clients.

Domain	Standards	Benefits & Rationale	Comments & Clarification
Assured data-at-rest protection	Requirement: Data stored on the device is satisfactorily encrypted when the device is in its “rest” state. For always-on devices, this is when the device is locked. Formal assurance of this function against the appropriate CPA Security Characteristic is necessary. http://www.cesg.gov.uk/servicecatalogue/CPA/Pages/Security-Characteristics.aspx	Implementing strong data-at-rest protection requires more than simply selecting a strong set of encryption algorithms. Independent assurance against the Security Characteristic results in enterprise confidence that the department’s obligations to protect information are being adequately met. The requirement set out in the Security Characteristic in relation to the use of a ‘simple’ or ‘smart’ token for the protection of the Key Encryption Key, is not currently achievable in all native disk encryption components. Such techniques allow shorter passwords for users - reducing likelihood of forgotten passwords. A Trusted Platform Module (TPM) can be used in place of a token, making the user experience smoother whilst providing a similar degree of cryptographic strength to the Smart Token method.	Currently, CPA assurance is required for the native Linux, Mac OS X and Windows 7 disk encryption technologies. The use of TPM is not mandatory, but can enable an elegant solution to protecting disk encryption keys. The case for requiring TPM will improve significantly when it has become widespread in consumer commodity markets. Where use of a smart token, simple token or TPM is not possible with a particular data-at-rest encryption component or product, a per-product or component decision as to whether the product could be used with a longer passphrase as a cryptographically sound interim option. This decision would need to be informed by cryptographic experts based on an understanding of the product in question.

Domain	Standards	Benefits & Rationale	Comments & Clarification
Authentication	User to device: the user is only granted access to the device after successfully authenticating to the device. User to service: The user is only able to access remote services after successfully authenticating to the service, via their device. Device to service: Only devices which can authenticate to the enterprise are granted access.		
Authentication: user to device	Implementation: Implementation method will depend on the platform and design of the data-at-rest encryption protection. The authentication of the user to the device may be inherent in the user's ability to unlock the device from its at rest state, or alternatively it may be the device's native login screen.		

Domain	Standards	Benefits & Rationale	Comments & Clarification
Authentication: user to service	Implementation: Authentication of user to services should be implementable with standard browser-based functionality. This could be as simple as HTTP forms, HTTP Basic authentication, or make use of open standards and services for passing identity assertions between services on behalf of a user, SAML for example. Services which contain or operate on sensitive data may require a stronger authentication of the user, for example, using a smart card or 2nd factor of authentication, as long as these conform to interoperability standards above.	For some services, simply the fact that the user is accessing the service from an enterprise device which they have authenticated to will be enough to grant the user access to the service, but for others it will be necessary for the user to authenticate to the service. Often it will be necessary for the service to audit which users accessed which data within the service, meaning that a strong identity assertion must be made to the service on behalf of the user.	The use of web authentication does not preclude single-sign-on user experience. This can be achieved through client side “keychain” mechanisms as is increasingly common in operating systems and browsers, or through the establishment of inter-service trust relationships making use of identity and trust brokers as envisioned by the PSN programme. The use of client side user certificates can make this process even smoother and transparent to the user once an employee PKI has been established.
Authentication: device to service	Implementation: X.509v3 device and gateway certificates which are validated as part of the IPsec IKEv2 mutual authentication handshake.	The requirement for device to service authentication (and service to device) is met through assured IPsec client and gateway configured in the assured configuration.	It is not expected that any service should require additional device authentication beyond the mutual authentication established by the IPsec IKE exchange.

Domain	Standards	Benefits & Rationale	Comments & Clarification
Secure boot	**Requirement**: An unauthorised entity should not be able to modify the boot process of a device, and any attempt to do so should be detected.	The enterprise and user will know that when their device is turned on that it boots into a secure state and provides a degree of confidence that it has not been compromised if it has been outside of the user's care.	Different platforms protect their boot chain in a variety of ways. The most appropriate mechanism for the platform will be identified in platform-specific guidance.
Platform integrity and application sandboxing	**Requirement**: The device can continue to operate securely despite potential compromise of an application or component within the platform, and there is an ability to restrict the capabilities of applications on the device.	The ability to sandbox an application and constrain the capabilities of the platform exposed to it means that confidence can be built in the platforms ability to protect applications processing enterprise data from less trusted applications. The extent to which the intrinsic integrity and application sandboxing capabilities of a platform can be relied upon will depend upon the extent of any platform assurance activities.	The common operating system access and permission controls, such as user or file based process permissions, can meet this requirement if well implemented. This requirement does not require that the Windows, Linux or Mac OS X operating systems require additional 3rd party application sandboxing tools.

Domain	Standards	Benefits & Rationale	Comments & Clarification
Application whitelisting	**Requirement**: The device can continue to operate securely despite potential compromise of an application or component within the platform, and there is an ability to restrict the capabilities of applications on the device.	Constraining the applications able to run on the device to an authorised set significantly reduces the ability for malicious code to execute. Only allowing a whitelist of applications to run, as opposed to using techniques which blacklist known malicious applications avoids the race to update the blacklist in response to a newly detected malicious application. Assurance in the application sandboxing and platform integrity aspects of the platform would allow a more liberal approach to approving applications to run on a device.	The common operating system access and permission controls, such as user or file based controls, can meet this requirement if well implemented.

Domain	Standards	Benefits & Rationale	Comments & Clarification
Malicious code detection and prevention	**Requirement**: The device can detect, isolate and defeat malicious code which has somehow become present on the device. Example methods for implementing this requirement are likely to include a combination of the following: • Anti-malware tools • Behavioural monitoring of applications and platform • File and URL reputation	Preventing code known to be malicious from reaching or executing on a device is a mitigation which has been employed on enterprise devices for some time. Such techniques are typically only a subset of modern security suites, and techniques such as URL reputation (where any file received from a known-compromised server is presumed to be malicious) provide good supplementary protection. The requirement to implement this control within the device should be considered on a per-platform basis, taking into consideration the use of application whitelisting and the strength of the native platform integrity and application sandboxing capabilities. It is also worth noting that the architecture assumed within this standard, whereby all untrusted traffic passes through enterprise controls, provides the ability for this control to be employed at an enterprise gateway rather than on the device.	Risks relating to malicious code will be mitigated in different ways on different platforms and the requirement for third party tools will be affected by the strength and configuration of other controls. This requirement could be met using network level gateway controls, implementing malware detection and content reputation filtering, requiring no additional controls at the device. It is good practice to provide defense in depth and implement light but effective controls for those operating systems where evidence indicates a higher risk from malware. Native tools are not excluded from such implementation, there is no specific requirement for 3rd party tools.

Domain	Standards	Benefits & Rationale	Comments & Clarification
Security policy enforcement	**Requirement**: Security policies set by the enterprise are robustly implemented across the platform. The enterprise can technically enforce a minimal set of security-critical policies on the device and these security-critical policies cannot be overridden by the user.	Just because a security policy mechanism exists within a platform it does not necessarily need to be switched on, as doing so can impair the user experience. Therefore, only the necessary security controls within the platform will be enabled. The controls deemed necessary for OFFICIAL information will be determined by technical security experts in CESG, usability representatives from Government and with support from the platform vendor where possible, to ensure the best supported and most elegant options of achieving the security goal are adopted. All platforms will be secured to mitigate the same set of risks for OFFICIAL information. In order to have confidence in the integrity of the enterprise device estate, the enterprise must have sole control over settings which implement security-critical features. Users may have control over non-security critical settings.	This requirement does not imply that a 3rd party security suite is necessarily required over and above a platform's native multiple device administration tools.

Domain	Standards	Benefits & Rationale	Comments & Clarification
External interface protection	**Requirement**: The device is able to constrain the set of ports (physical and logical) and services exposed to untrusted networks and devices and any exposed software is robust to malicious attack. Implementation: Network interfaces are protected by a host-based firewall configured to prevent inbound-initiated network connections to the device and limiting outbound-initiated connections to IPsec VPN gateway only on the required ports. Physical and wireless interfaces only allow a whitelist of allowed peripherals to connect and communicate with the device using specific protocols.	One of the most likely attack vectors against the device is malicious content delivered to the device through a path which does not transit the defences within the enterprise. Such an attack could be borne by physical devices such as removable media connected directly to the platform, or remotely attack through a wired or wireless interface. Filtering web-based content or file-based content within the enterprise rather than on the device means it can be achieved more robustly, subject to stronger audit and monitoring.	This requirement does not imply that a 3rd party security suite is required.

Domain	Standards	Benefits & Rationale	Comments & Clarification
Device update policy	**Requirement**: Security updates can be issued by the enterprise and the enterprise can remotely validate the patch level of the device estate.	Applying security patches to devices for known vulnerabilities is necessary to keep those devices from being vulnerable to attack.	This requirement does not imply that a 3rd party security suite is required.

Domain	Standards	Benefits & Rationale	Comments & Clarification
Event collection for enterprise analysis	**Requirement**: The device reports security-critical events to an enterprise audit and monitoring service. The user is prevented from tampering with the reporting of events from the device. Implementation: Only security-critical events which can only be collected from the device are required to be logged and reported to an enterprise-based audit service. Such events will include: • User log in and log out • Local security alerts from third-party tools or platform components such as alerts from anti-malware, host-based firewall, platform integrity checks which fail. Accurate time is required for audit, time on devices should be maintained through an NTP hierarchy which chains to common PSN time services.	There is a general preference for collecting audit events from the enterprise services wherever possible and only collecting security-critical events from devices which cannot be collected elsewhere. Events should be fed into an enterprise audit and monitoring service designed in accordance with CESG Good Practice Guide 13 (GPG 13). This standard makes no provision for auditing for legal compliance or evidential requirement. Where such a requirement exists it will need to be considered by the implementer.	It is important to apply proportionality to event logging. In addition to user session logging, only exceptional security related events or alerts are required to be logged. That is, events which indicate a breach of security policy or triggering of a security control or mitigation. The emphasis on event logging should be at the remote service, not at the device. Logging of the same events should not be duplicated between a device and elsewhere.

Domain	Standards	Benefits & Rationale	Comments & Clarification
Incident response	**Requirement**: The enterprise has a plan in place to respond to and understand the impact of security incidents, such as the loss of a device. This should be supported by appropriate functionality within the devices and the enterprise, such as sending a wipe command to the device and revoking credentials. Implementation: A response plan should be in place to deal with loss or compromise of the device in line with the advice set out in GPG 13. Such a response plan should include revocation of the device certificates and user credentials.		This requirement can be met entirely using procedures and actions that do not require additional software or tools to be implemented in the device. For example, revocation of access and authentication privileges can and should be undertaken at the backend. This requirement does not necessarily imply that a user's login is disabled locally at the device, nor does it imply that a device must be remotely wiped. It is sufficient to revoke access privileges to all enterprise services and information.

Security Scenarios

Scenario	Outcome
Loss of laptop in public place.	The user reports their laptop as missing as soon as they notice by calling their IT helpdesk. The helpdesk follows the Incident Response Plan. Lock or kill message sent to device. The device certificate is revoked. User account is locked and audited to ascertain if departmental services have been compromised. Since data-at-rest protection was assured against the CPA Security Characteristic then cryptographic attacks to recover the disk encryption key, even using large-scale computing resources is impractical. The principle of limiting data stored locally on the device will help to reduce potential impact of laptop loss.
A malicious document is received as an attachment to a socially engineered email.	Incoming email is scanned through enterprise-class mail scanning service where most known malware can be detected and removed. In the event that the email reaches the user, they have been trained to be suspicious of receiving unexpected email from unknown sources so do not open the attachment. The IT helpdesk follows their Incident Response Plan to perform any post-incident analysis.

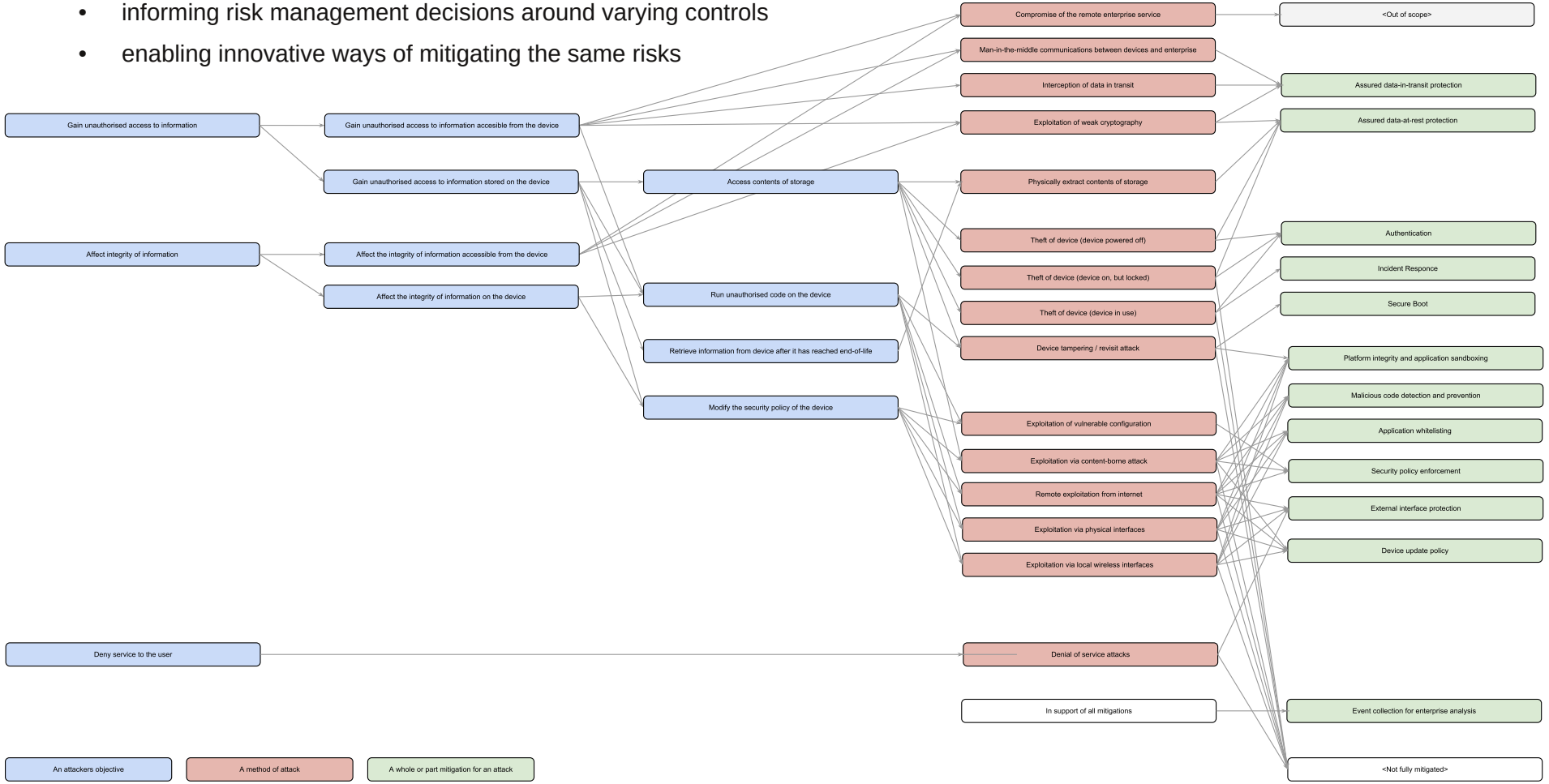
Scenario	Outcome
A malicious document, intended to compromise the desktop application which renders it, is downloaded from the Internet. The exploit payload attempts to exfiltrate files from the device to a remote location.	The reputation of the server which the document is stored on is flagged as untrustworthy within the browser. If the file is not flagged as suspicious due to its source, then as it is downloaded it will pass through enterprise gateways. Running the latest version of the client-side application software is the strongest defence against exploitation from known vulnerabilities. Other platform integrity measures or application sandboxing will also limit the impact of a compromised application.
A user receives a link to a malicious site, masquerading as a legitimate site. Banking, shopping, social media and email are amongst target sites for such 'phishing' attacks.	Enterprise gateways will prevent access to sites known to be part of such 'phishing' attacks. This measure may be augmented by in browser reputation based filtering.
User is personally threatened to extract device login credentials.	Device access is compromised by attacker and access to OFFICIAL information is obtained. The user reports the incident to their helpdesk which follows the incident response plan. Access to sensitive data requires the user to utilise a 2nd factor of authentication not available to the mugger, so the impact is limited and enterprise-side auditing allows the department to ascertain the extent of the information compromised.

Scenario	Outcome
Some public Internet web applications require access over SSL or TLS. This has the potential to undermine enterprise protection of the devices.	The corporate gateways proxy the SSL connection allowing the traffic to be inspected to ensure the device is not compromised through the encrypted tunnel and that OFFICIAL information is not being leaked from the device over the encrypted tunnel.
Employee wishes to use the EUD to undertake personal online banking.. The department wishes to allow the employee to verify that they have an end-to-end encrypted session with their bank.	The proxying of the SSL/TLS tunnel is bypassed for a whitelist of banking sites, subject to departmental risk management where it is thought that the service present minimal risk to the departmental devices.
Access to a web-based application for accessing OFFICIAL Sensitive information.	The web application prompts the user to provide additional credentials for stronger authentication, such as a one-time code or a smart card. Aggregation of OFFICIAL-SENSITIVE material on the EUD is mitigated by a combination of (1) periodic removal of application caches on the device, and (2) use of remote viewing which minimises transfer of content to the EUD, (3) local storage limits for EUD devices, (4) server side rate and quantity limiting access.

Traceability for Threat, Attack Method and Mitigation for OFFICIAL Information

The following schematic provides traceability between threat actor objective, means of attack, and mitigations, as appropriate for mobile devices accessing OFFICIAL information. This transparency is useful for:

- justifying security controls
- informing risk management decisions around varying controls
- enabling innovative ways of mitigating the same risks



Remaining Assurance Activities

The following table summarises the current availability of VPN and disk encryption products assured under the Commercial Product Assurance scheme, highlighting the remaining assurance activities to enable the use of Linux and Mac OS X for mobile end user devices:

Platform	VPN Client	Disk Encryption	Platform Assurance
Windows 7	Windows 7 native client CPA assurance requires sponsorship	Windows 7 native and 3rd party products assured	Configuration guidance available from CESG (Government Assurnce Pack)
Apple Mac OS X	Native VPN client not capable of IKEv2 - needs update from Apple. IKEv1 permitted as an interim mechanism, but still requires CPA. Open Source IPsec client CPA underway.	Filevault native tool CPA assurance requires sponsorship	Subject to prioritisation by CESG
Linux	Open Source IPsec client CPA underway.	dm-crypt/LUKS native tool CPA assurance requires sponsorship	Subject to prioritisation by CESG

Platform assurance will result in further operating system specific configuration guidance from CESG, likely enabling further flexibility in the use of such devices. Until that has been delivered, devices with operating systems that have not yet received platform assurance, should only used to access uncaveated OFFICIAL information.