End User Device Strategy: Design & Implementation

This document establishes the technology, commercial and security principles for designing infrastructure to implement the End User Device Strategy.

Together with accompanying detailed definitions of the interoperability and security standards, it can be used to ensure departmental change programmes are aligned to government IT strategy. It can also be used by spend control and architecture review functions to ensure proposals for change are aligned.

Context

The Government ICT Strategy 2011 actioned the development and implementation of an End User Device Strategy to address historic issues including user tools that do not meet user needs, degrade productivity and do not provide a pleasant user experience. These are compounded by overly expensive end user devices and associated services, high costs or even inability to change user IT to meet user needs, a growing divergence from the modern user-friendly consumer IT being exploited in other sectors, and an entrenchment of incumbent products and suppliers through technical and commercial dependencies or “lock in”.

The Civil Service Reform Plan requires departments to address “frustrating” IT tools for civil servants. Its Workplace Transformation programme will streamline working practises, supported by effective IT.

The Government Protective Marking Scheme Review and resultant Security Classification Policy, and the Open Standards policy require a reform of the principles by which IT tools for civil servants are designed, procured and managed. Civil servants are expected to take responsibility and apply reasonable judgement when dealing with information, removing the need for overbearing technical controls.

The Government and Departmental Digital Strategies establish user needs as the central focus of digital services and tools. This requires a step change in agility to meet those user needs, together with an excellent user experience.

This guidance for implementing the End User Device Strategy is key to delivering all of these ambitions.

Vision

The strategic vision for end user devices is as follows:

- **User choice** to select the device best suited for their role or task currently offered by the market, and to change that choice easily.

- **User experience** as a central goal in the development of IT solutions, properly balanced against integration and management requirements.
- Highly **dynamic market** for the supply of end user devices achieved through no dependency between devices and applications or services, no exclusivity over supply, and a clear transparent specification implementable by suppliers of all sizes.
- A **level playing field for open source**, providing competition and potentially better value.
- Both devices and services designed and built from successful ecosystems: the **consumer commodity IT** market, **cloud** services and the **public internet** with its open standards and technologies.
- Applications and services designed to make no assumption about end user device brand, vendor or supplier, with no requirement to customise the basic devices to consumer applications. The device is **decoupled** from applications, services or other middleware.
- **Commercial grade security** reflecting the threat model for OFFICIAL information, with no bespoke controls, and security critical functions met through assured commercial products. Greater interoperability of IT systems through a common approach to securing OFFICIAL information.
- **No exclusivity** over the supply of devices or associated services. Instead, a compatible mix of end user devices and services, made possible through decoupling applications from devices.
- **Transparency** into costs and performance enabling informed customer choice.

Transition

It is expected that most Departments will require incremental change to achieve alignment with this strategic vision.

Opportunities for concrete steps towards implementing this strategy include:

- **Architectural reconfiguration** of existing IT infrastructure, such as the development of platforms or service lines, including desktops or end user computing. This can include reimaging existing hardware assets.
- **Large scale re-procurements** of IT services including end user computing and devices.
- **Localised changes** to applications, middleware services, end user devices or desktops, including new deployments or refreshes. Investment in upgrades must also trigger an evaluation of strategic alignment.

Departments must ensure that at the end of any current wholesale IT outsourcing contracts, they are optimally positioned to consume disaggregated commodity services.

Activities to aid strategic transition will include:

- **User needs** - identify user needs through direct engagement, and understand user

groups within the organisation.

- **Security** - understand the information security constraints for those users, challenging any over-assessment, and requiring justification for non-standard requirements.
- **Business outcomes** - discipline any change effort by confirming clear business outcomes, organisational and strategic.
- **Commodity and innovation** - define the IT service elements required, aiming to consume commodity services, but recognising where innovative elements are genuinely required.
- **Architecture** - define the strategically aligned technical and commercial architecture. This will include consideration of open standards, modular design, cloud services, a level playing field for open source and SME suppliers.
- **Transformation** - Execute the activities required to achieve the architecture. This may involve the disaggregation of IT services including contract adjustment, implementation of open standards and interfaces, redesign of security controls, and re-procurement of services from a wider market.
- **Agile pilot** - Significant change is best delivered iteratively, starting small and growing, with continuous feedback from users.

The spend controls function of the Cabinet Office will support Departments towards strategic alignment.

Scope

The End User Device Strategy is applicable to central Government departments including their agencies and related bodies, operating at the OFFICIAL security domain.

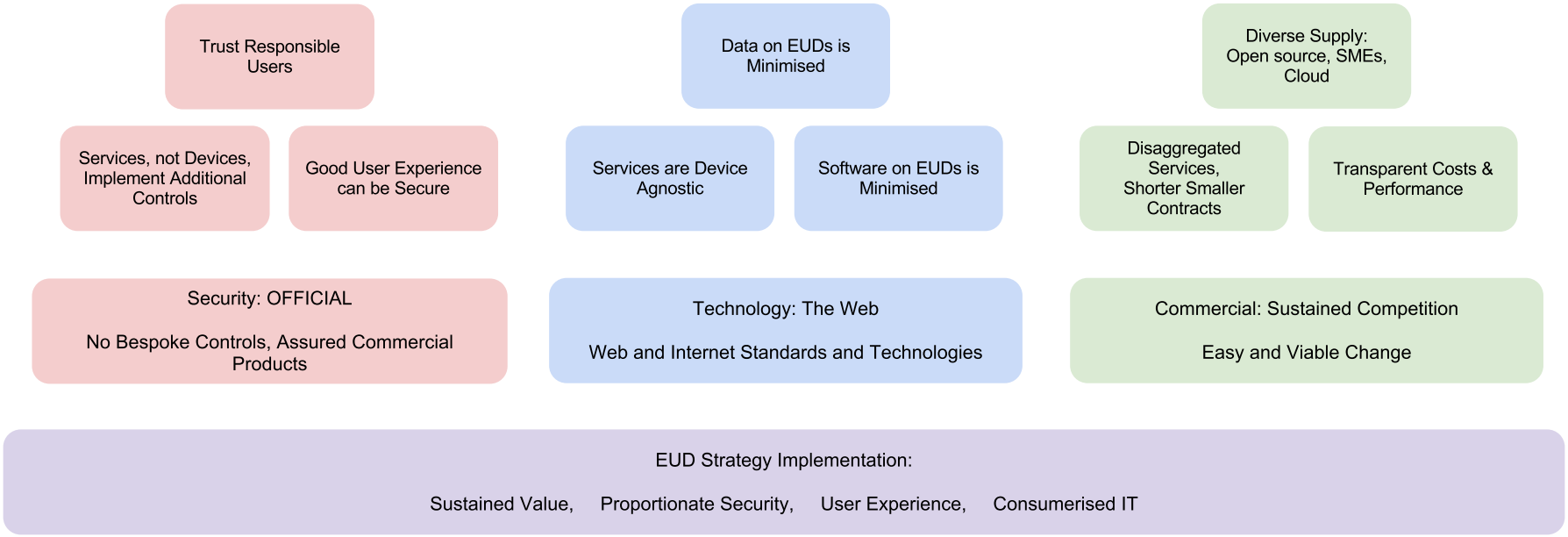
Detailed guidance for mobile laptops has been issued, with forthcoming guidance for mobile phones, tablets and other form factors.

Guidance

This note forms part of a set of guidance issued by the Cabinet Office:

1. A **briefing for senior leaders** clarifying strategic direction and proving an update on new implementation guidance.
2. High level **transition and implementation principles** for the End User Device Strategy. These govern the commercial, security and technology design for departmental implementation, and are critical to deliver the strategic vision.
3. Detailed guidance on **interoperability standards** to which end user devices are expected to conform.
4. A modern **security framework** for mobile end user devices including laptops, tablets and smartphones. The guidance makes clear the balance between user experience, costs, complexity and a dynamic supply market.

EUD Design & Implementation Principles



EUD Design & Implementation Principles

The primary implementation goals for the End User Device Strategy are:

1. **Sustained Value**. To ensure value, the market for End User Devices must be dynamic and competitive. Barriers to a market without sustained competitive tension must be removed. Typically this means that there must be no lock-in between the user device and applications or services, no barriers to a wide range of suppliers including SMEs and those proposing open source solutions. Transparency into costs and performance are key to informed customer choice. An easy and viable ability to change suppliers is key to sustain competitive tension over suppliers beyond the point of purchase.

2. **Proportionate Security**. Security controls will be justifiable and proportionate to the OFFICIAL threat model. Security controls will be commercial grade, sourced from the commercial market, and there will be no bespoke government-only controls. There will be a greater emphasis on user responsibility, reducing technical controls, but supported by better auditing to verify users are acting responsibly. The user experience must be such that users don't want to circumvent the controls, or find their productivity degraded.

3. **User Experience**. User needs and experience are critical to the value of any IT system. End user devices and their use must meet user satisfaction, and not merely pass traditional corporate criteria for procurement or security.

4. **Consumerised IT**. The large scale and highly successful ecosystems of consumer commodity IT and the public internet offer both value for money and minimised technical risks. This is the principle of "copying successful models". End user devices should be sourced from consumer commodity markets and configured, not customised. Niche supply and bespoke builds are risky and offer low value. This principle also means adopting public internet standards and technologies where they have proven to be open and adopted by a wide range of consumers and developers. Often these are lighter than heavier enterprise offerings.

Technology Principle 1: The Platform is the Web

The public internet, world wide web and online digital services are an immensely successful ecosystem and economy. It is scalable and robust, it is a platform for innovation open to many kinds of businesses and communities, and fierce competition rewards services that meet user needs, driven by technologies and methodologies that work and are attractive to real world developers.

End user devices and associated infrastructure should mirror the best practices of the web ecosystem. This means:

All applications and services are accessed through a modern standards compliant web browser. Today there is little reason not to use the web as very rich user experience can be achieved using common internet technologies.

Standards and technologies for the web only succeed if they are light, both user and developer friendly, and open to the widest range of developers, businesses and communities. This is in contrast to traditional enterprise IT promoted by a small set of mostly large businesses, and selected by corporate IT departments on behalf of end users.

Applications and services are developed for the widest possible user base, with no assumption about current or future end user devices. This means applications are not designed for a specific browser, operating system, or device.

Web approaches, meaning browser based approaches, are preferred. Where this is not appropriate, broader internet approaches are acceptable. To illustrate this, an email service should be accessible through a web browser and ideally expose HTTP interfaces. Where this is not appropriate, with mobile phone native mail applications for example, the established and open SMTP, IMAP internet standards should be used. Proprietary single-vendor interactions do not reflect this principle.

Technology Principle 2: Services are Device Agnostic

Strengthening the web principle, all services will be agnostic to the device that is used to access them. This means there can be no assumption of any specific vendor or supplier of the end user device. Specifically this means that the applications and services should not use functions which are beyond the common open standard and only implemented by a specific vendor or supplier.

This also means that applications and services should adapt gracefully to the end user device’s form factor or hardware capabilities as is best practice amongst leading digital services.

Furthermore, there should be no significant degradation of user experience between equivalent devices leading to preferred devices or vendors, nor a separation into tiers of first and second class users.

Services will be developed as “pure web” applications. This means they will employ open standard and common web technologies requiring only, and any, modern web browser. Modern HTML and its associated technologies can provide for a rich user experience.

Platform or vendor specific extensions, such as ActiveX controls, are not permitted. Technologies which are relatively cross-platform such as Java or Flash are not part of the strategic vision and their capabilities are increasingly implementable using pure web technologies.

Where there is a need for locally installed applications, these should interact with other services and systems using open standards.

Technology Principle 3: Software on EUDs is Minimised

End user devices will remain simple. Their initial design will minimise 3rd party software, and avoid duplicating functions that are available with the underlying operating system. Furthermore, accumulation of software or configuration over time will also be minimised.

This reinforces the principle of pure web applications requiring no locally installed components, extensions or plugins, and keeping the devices as simple as possible to enable easier support and changeability.

Technology Principle 4: Data on EUDs is Minimised

End user devices must never be the authoritative source for business information. Such business information may be temporarily cached at an EUD, but will be primarily stored away from the EUD, in corporate or cloud storage repositories. This implies server side working, or sufficiently frequent synchronisation. Data should not be permitted to aggregate on a device.

These measures significantly reduce the cost and complexity of maintenance. Lost or broken devices can simply be replaced. They also aid efficient information management, meeting security and regulatory requirements.

This principle extends to applications, which should primarily be licensed per role and by device. This means users can roam between devices without incurring additional application licensing costs. The exception to this approach is the use of rarely used applications which can be associated with a specifically designated shared device.

Commercial Principle 1: Sustained Competition

The key to long term value is to sustain competitive tension beyond the point of purchase or deployment. This means the suppliers do not enter into a monopolistic or dominant position once a supplier has been selected. Critical to sustained competitive tension are genuine alternative solutions from different suppliers, and the required transition itself being viable. In addition to technical flexibility, the commercial arrangements must also support the ability to change to alternative solutions and suppliers.

Contracts which transfer away design responsibility, penalise change or grant exclusivity are not aligned to this principle. Many smaller and shorter contracts are preferred over larger longer contracts.

The common commercial strategy of aggregating demand to attract discounts for volume purchasing is not sufficiently sophisticated as it does not sustain competitive tension beyond the point of purchase. Potential monopolistic or dominant supplier tendencies are not addressed by this strategy. Negotiations with suppliers are not backed by the ability of a customer to choose an alternative solution.

A key factor in the ability to change suppliers is avoiding bespoke or customised solutions and services, instead adopting the discipline to procure commodity and consumerised services, for which there is both a large dynamic competing user-focussed market and the ability to change suppliers with relative ease.

Commercial Principle 2: Disaggregated Services, Small Short Contracts

Large contracts which cover many service or technology domains suffer from several issues which ultimately degrade value and experience for the customer. For example, such contracts suffer from a lack of transparency into component costs with the resultant inability to benchmark or compare costs.

Suppliers which have gained extensive control over a customer’s infrastructure potentially have undue influence on both the business and technology functions beyond their contractual remit.

An important key benefit of multiple smaller contracts over fewer larger contracts is that business functions are broken into smaller components, reducing both delivery risk and also the impact of a component or service failure. Furthermore, such disaggregation opens access to a wider range of suppliers, some of them smaller businesses offering much better value for money, greater specialisation and agility than many large suppliers.

This principle is sometimes challenged as there is a theoretical cost and complexity overhead of reconstituting disaggregated services. In reality, the loss of value from not disaggregating services is far greater than this potential overhead.

Contracts will be smaller in scope, and shorter in length. A useful indicator of appropriate

granularity is to select the smallest contractual scope for which there is a market of alternative suppliers. There must be a presumption against contracts larger than £100m and longer than 2 years in duration.

Furthermore, contracts must not grant exclusivity of business to any supplier. Overarching contracts must allow a diversity of suppliers for constituent services. Similarly, contracts must not penalise strategically aligned change. Amongst the worst examples of this are contracts which require compensation to a supplier for loss of business in the case that business transferred to an alternative supplier.

Commercial Principle 3: Transparency into Costs & Performance

Suppliers must provide transparency into costs ultimately paid for by the customer. This means open book accounting and full auditability. It also means such accounts are publicly published for taxpayers to judge value, and to drive positive supplier behaviours.

There must also be a step change in the reporting of performance. This means clear unambiguous and relevant definitions for performance metrics. The performance of a supplier should not be monitored and reported by that same supplier.

Historically some suppliers have charged customers additional contingency or risk costs for IT solutions which were not their preferred options. Departments must drive suppliers to justify such costs through transparency into their formulation. This leads to reduced costs as such risks become better qualified, or are resolved by alternative suppliers.

Commercial Principle 4: Diverse Supply

Departments must be open to the best value solutions from a wider range of suppliers. This means being open to types of business model and technology solution beyond those traditionally entertained. This means removing barriers to open source solutions, working efficiently with SMEs, and adapting to accommodate services sourced from the cloud.

A diversity of suppliers and solution types adds healthy competition and innovation to the markets departments buy from.

Security Principle 1: Assured Commercial Solutions for OFFICIAL

The Security Classification Policy makes clear which information should be considered as OFFICIAL. This will include the large majority of government information, including some that was previously marked as RESTRICTED or even CONFIDENTIAL.

OFFICIAL information is subject to commercial grade threats which can be mitigated with appropriately assured commercial grade security controls. This means security controls and mechanisms are sourced from the commercial market, and are comparable with the best practices of large well run private sector companies. The Commercial Product Assurance scheme is appropriate for providing the required level of assurance for security enforcing functions for OFFICIAL. This scheme obviates the need for bespoke government-only controls for OFFICIAL.

Security Principle 2: Services, not Devices, Implement Additional Controls

End user devices which adhere to the OFFICIAL Security Framework provide sufficient security for accessing and working with OFFICIAL and OFFICIAL-SENSITIVE information. It is not expected that access to different services or information would require additional controls on top of those in the framework to be levied on the end user device; any such requirements should always be challenged to ensure they are strictly necessary.

Where there is a legitimate additional requirement to control access to more sensitive information, controls should to be implemented within the service, rather than the device.

Over time this enables the freeing of devices and services from organisation-wide blanket security controls, reducing complex dependencies, and enhancing the ability to change systems and suppliers. In many cases this architectural approach reduces costs because a single well implemented security layer for an application can be cheaper to develop and maintain than a distributed set of controls extending over many and potentially diverse EUDs.

A legitimate example of additional requirements might be the need for 2-factor authentication for specific services. Such authentication must be designed and implemented avoiding any changes or further requirements (hardware or software) on the EUD. Web or SMS based channels for confirming 2-factor authentication are good options to consider.

Security Principle 3: Good User Experience can be Secure

Security and good user experience don’t need to be mutually exclusive. Modern intelligently designed security can often be made largely transparent to the user, whilst also providing the enterprise with the confidence it needs that its information is suitably managed.

Experience confirms that degraded user experience often leads users to circumvent the security controls by employing less secure unofficial IT solutions. Users who retain the provided IT systems suffer degraded productivity. The outcome is that security is not

maintained and user experience is degraded.

Where some degradation of user experience is unavoidable, a risk management analysis must consider the negative impact of users avoiding unpleasant official IT and degraded productivity.

Security Principle 4: Trust Responsible Users

Users should be trusted to carry out their roles and given the responsibility to do so securely. Audit and verification of user behaviour should be used to ensure policy compliance instead of preventative measures which add cost and degrade productivity. Such audit and verification should be implemented by services or network infrastructure, away from the end user device.

Departments should invest in security controls to defend individual users against threats that they themselves cannot reasonably defend against. Such threats are usually from moderately capable sources such as activists, journalists and criminals operating online.

Departments should not invest in security controls to defend against risks that a responsible individual can reasonably be expected defend against. Examples of such scenarios include not working on sensitive information in an open busy public place, or exercising reasonable judgment about which information is sent to external recipients by email over the public internet.

This approach is possible because Departments will ensure that only suitably trained and vetted staff are employed and given access to OFFICIAL information.

This stance leads to reduced technical controls and their associated costs, whilst also optimising the usability and flexibility of the IT tools for the majority of responsible users.