



MINISTRY OF DEFENCE

Ministry of Defence

Defence Identity and Access Management Strategy 2010

A sub-strategy of the MOD Information Strategy





MINISTRY OF DEFENCE

Defence Vision

To produce battle-winning people and equipment that are:

- Fit for the challenge of today
- Ready for the tasks of tomorrow
- Capable of building for the future

Defence Information Vision

Agile exploitation of our information capabilities to improve effectiveness and efficiency on operations and in support areas through access to, and sharing of, timely, accurate and trusted information

Defence Identity and Access Management Vision

A federated identity and access management capability that enables trusted access to, and secure sharing of, information by our people and partners across operational, support and business areas

Identity and Access Management Transformation Goals

Goal 1: Deliver identity management capability to manage the digital identities of all MOD people

Goal 2: Provide all MOD people with a single, trusted credential for identification and access to required logical and physical resources

Goal 3: Provide an automated provisioning capability with self-service facilities

Goal 4: Deliver a logical access management capability for MOD and trusted partner users

Goal 5: Implement an Information Handling Model (IHM) across all domains

Goal 6: Enable secure information sharing with partners through federation

Goal 7: Implement an integrated physical access management capability

Goal 8: Exploit identity and access management capabilities to realise operational, business and financial benefits

Contents

Foreword	2
Prelude	3
The Case for Change	6
Defence IdAM Transformation	11
Delivery of the Strategy - Next Steps	15
Annex A - Definition of Terms	16
Annex B - IdAM Transformation Goals	18
Annex C - IdAM Benefits	23

Foreword by Defence Chief Information Officer



The MOD Information Strategy (MODIS), published in 2009, provides a framework to support the reform of Defence information capability and establish the conditions to achieve the Defence Information Vision. The Defence Identity & Access Management Strategy (IdAM) 2010 is one of a number of sub-strategies that make up the information reform roadmap. One of the MODIS guiding principles is that “Information has more value when it is shared securely”. Delivery of the IdAM strategy will enable appropriate information sharing within MOD, with the rest of Government, and with external partners, by allowing the right people in the right places to gain the right level of access to the right information at the right time.

This strategy defines the components of an IdAM capability and outlines why IdAM is important to Defence; it presents the case for change; the vision, guiding principles, trust model and strategic goals to realise the reform, including its costs and benefits, and the next steps to deliver the strategy.

My team has developed this strategy in consultation with TLBs and partners. It is designed to drive forward MOD’s contribution to Government identity initiatives and is aligned with relevant external initiatives such as the Combined Communications-Electronics Board (CCEB) Public Key Infrastructure (PKI) Interoperability Architecture and Transglobal Secure Collaboration Program (TSCP) strategy.

We will work with stakeholders, including the owners of the strategic goals, personnel and security organisations, TLBs and partners, to deliver the strategy. The first step will be to develop a roadmap. This will seek to deliver the IdAM capability incrementally, with priority given to delivery of quick wins and changes that realise the biggest benefits. We will examine the feasibility of conducting pilots to test solutions before commitment.

I believe that modernising the way that we manage and use identities and credentials to control access to resources is crucial to enable trusted collaboration and secure information sharing across Defence, and hence help realise the goal of Information Management excellence. I commend this strategy to you and look to your support in taking it forward.

A handwritten signature in black ink, which appears to read "John Taylor". The signature is stylized and cursive.

John Taylor, CIO

Prelude

What is Identity and Access Management?

Identity and Access Management (IdAM) is an integrated set of policies, processes, standards and technologies that:

- Creates and manages digital identities and associated access privileges for all people and other entities (e.g.; devices, applications, services or processes) within an organisation over the whole life-cycle.
- Binds those identities to credentials, such as smart cards or security tokens, for use in access transactions.
- Uses the credentials to control access to resources.

A definition of terms is provided at Annex A.

What is Identity Federation?

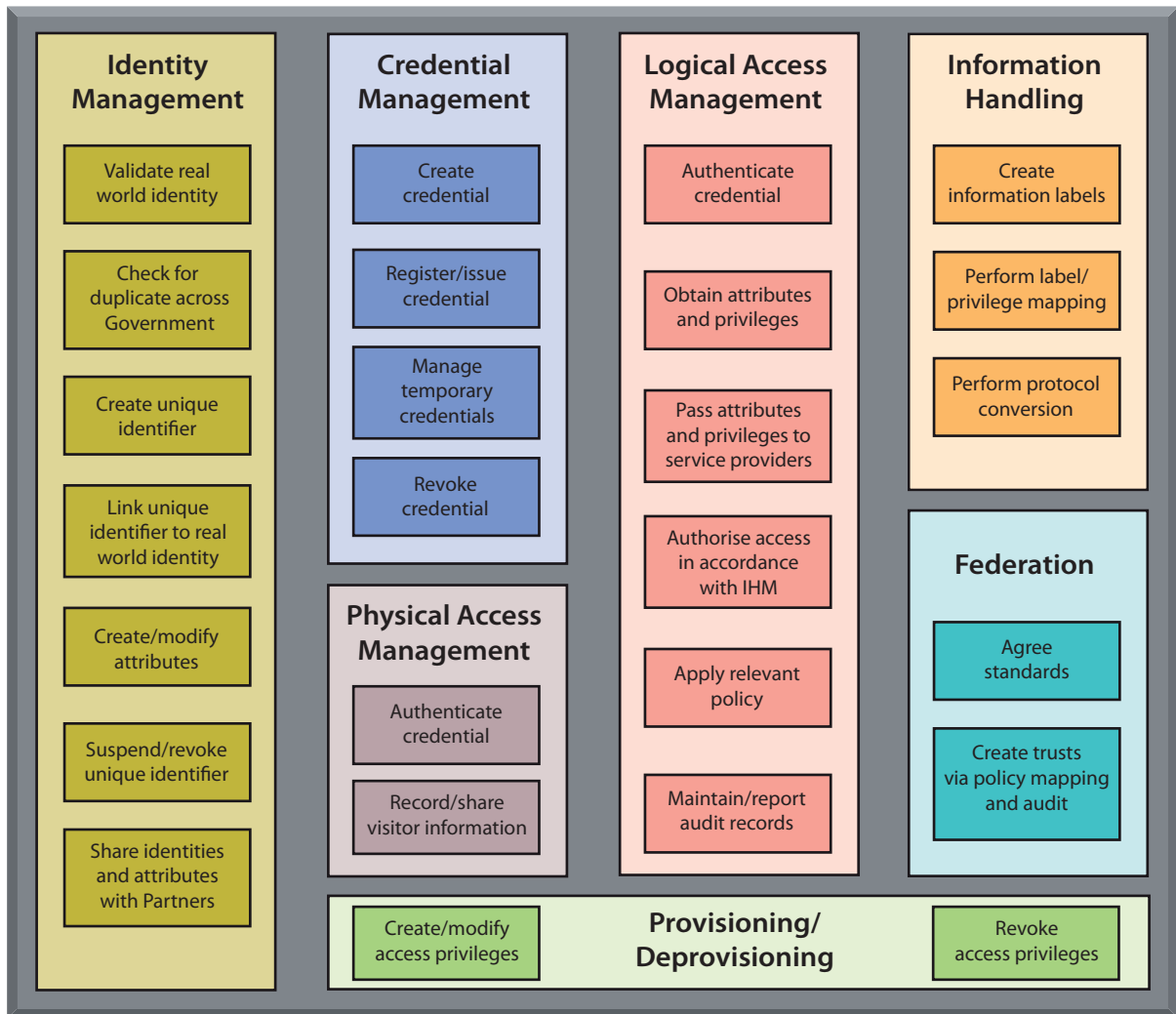
Federation means that identities and privileges are portable across autonomous boundaries, enabling authenticated users on one system to securely and seamlessly access information and services on another system without re-authentication. For MOD, it would enable single sign-on to information services across Defence, and secure information sharing with partners.

IdAM Capability

A federated IdAM capability, illustrated in Figure 1, consists of seven main components:

- Identity Management - Policies, procedures, standards and technologies for creating, maintaining, using and safeguarding identity information over its life-cycle.
- Credential Management - Policies, procedures, standards and technologies for creating, issuing, managing and revoking credentials, including in-field facilities to deal with lost, damaged, forgotten or expired credentials.
- Provisioning / De-provisioning – Policies, procedures, standards and technologies for creating, modifying and revoking access privileges. Once digital identities have been created, the rest of the process may be automated. When automated provisioning is in place, user self-service can be implemented.
- Logical Access Management - Policies, procedures, standards and technologies to control access to information services by authenticating credentials, authorising access to resources and applying relevant policies.
- Information Handling – Underpins the logical access management component by providing guidance on how identities, permissions, information attributes and business rules are related to control information access. It includes labelling policies and standards, and technologies for performing protocol conversion.
- Physical Access Management - Policies, procedures, standards and technologies to control access to buildings and sites by authenticating credentials and authorising access to facilities.
- Federation - The agreements, standards, and technologies that enable identities and associated access privileges to be shared across autonomous boundaries, and allow authenticated users on one system to securely and seamlessly access information/services for which they are approved on another system without re-authentication.

Figure 1 - Identity and Access Management Capability



Why Is IdAM Important to MOD?

A Defence IdAM capability would provide:

- Facilities for MOD users, both within and outside the MOD boundary, to gain secure access to trusted MOD information resources.
- Facilities for MOD to share information securely with the rest of Government and external partners.
- A single trusted source of identity information that can be used across Defence, avoiding duplication and inconsistency.
- A reliable source of corporate data about all MOD people including contractors and affiliates who regularly work within MOD but are not captured in MOD Human Resource (HR) systems.
- Automated provisioning and de-provisioning.
- Facilities for business users to conduct life-cycle management of identities.
- Self-service facilities for re-setting passwords and requesting/activating change.
- A single credential for identification and trusted access to logical and physical resources.

- Consistent application of policy to control access to information.

Benefits of IdAM

The main benefits of a Defence IdAM capability are:

- Easier collaboration and information sharing with allies, the rest of Government and industry partners
- Reduced information risk
- More agile, flexible and productive workforce
- Better management of identities and privileges
- Increased physical security
- Improved compliance with policy and legal requirements
- Better value for money (vfm)

The Case for Change

Strategic Context

This strategy directly supports the 2009 MOD Information Strategy (MODIS) [1]. One of the MODIS guiding principles is that "Information has more value when it is shared securely". Delivery of the IdAM Vision will enable appropriate information sharing within MOD, with the rest of Government, and with external partners, by allowing the right people in the right places to gain the right level of access to the right information. MODIS provides high-level guidance to support transformation of Defence information capability and establish the conditions to achieve the Defence Information Vision. This is one of a number of sub-strategies that make up the information transformation roadmap; it complements the MOD Information Assurance Strategy [2] and its delivery will make a significant contribution towards realisation of the goals within the Accessibility and Trust quadrant of the MODIS balanced scorecard, and play a part in realisation of the goals in the other three quadrants (Strategic Alignment, Information Exploitation and Value for Money).

This strategy is aligned with relevant cross-Government initiatives including the 2009 Safeguarding Identity Strategy [3], which sets out the Government's approach for establishing, using and protecting identity information of citizens; Requirements for Secure Delivery of Online Public Services (RSDOPS), which provides requirements for, amongst other things, identity registration, authorisation, authentication, privacy and information access; and the emerging Government Employee Identity Management Strategy [5], which defines the vision and roadmap for delivery of a capability to provide any Government employee with access to appropriate information and services from anywhere within or outside Government. MOD is contributing to development and delivery of these strategies and the underpinning policies, procedures, standards and technologies.

This strategy is aligned with relevant external initiatives, such as the Transglobal Secure Collaboration Program (TSCP) [6]. This is a cooperative forum of leading US/European aerospace and defence companies and government agencies¹, working together to develop open-standards based specifications that enable secure collaboration and assured information sharing between parties.

Current IdAM Capability

Significant elements of an IdAM capability are in place or planned. This section identifies these elements and indicates where further development is needed.

Identity Management

We have an emergent Identity Management (IdM) capability today, and this will be enhanced when planned DII software releases are delivered. Key components include the MOD's two HR systems, the Joint Personnel Administration (JPA) system for military personnel and Human Resource Management System (HRMS) for civilian employees; the Person Unique Identifier (PUID) database; d-Directory / e-Directory; DII Active Directory; and the Defence Public Key Infrastructure (PKI) service. However, if these are to form part of a coherent IdM capability, the following issues need to be addressed:

- JPA and HRMS are the authoritative sources for identity information on MOD employees and provide feeds to other systems. However, the information currently provided to other systems is inadequate to identify a person.
- There is no authoritative source for identity information on MOD people who are not employees. As part of the PUID creation process, information about non-employees is entered in a Contractor Database (so-called, but covers all affiliates such as staff from other UK Government Departments). The information in this database is inadequate to identify a person.

¹ As at July 2010, TSCP members include BAE Systems, Boeing, EADS, Finmeccanica, Lockheed Martin, Northrop Grumman and Raytheon, plus Government agencies from France, Italy, Netherlands, UK and US. NATO is expected to join in September 2010.

- An individual often has more than one PUID. This arises in the following scenarios:
 - Serial PUID Issuance: If a person serves in the armed forces then leaves and subsequently joins the MOD as a civil servant or contractor, or a contractor leaves and at a later time takes up a new contract, the person is likely to get a new PUID.
 - Concurrent PUID Issuance: This occurs when a person belongs to two organisations concurrently, such as a MOD civil servant or contractor who is a reservist.
- Life-cycle management of identity information is poor or non-existent:
 - Information in the PUID and Contractor databases is inadequate for life-cycle management (e.g.; there is no facility to tag an identity with its status, such as active or retired), and identities do not have owners or managers.
 - There is no rigour associated with maintenance of some identity repositories, such as d-Directory or DII Active Directory, so information can be woefully out of date; individuals often retain access permissions long after they should have been revoked, with financial and security implications.
- We have many systems and applications that hold identity information, resulting in duplication, inconsistency, inefficiency and risk.
- We have limited capability to manage the identities of devices.

Credential Management

Currently, there is no MOD trusted credential for identification and access to resources. Military personnel are issued with a Defence ID Card (MOD Form 90), a simple plastic ID card for use in face-to-face identity checks. There is a wide variety of building passes in circulation, typically a plastic card printed with the name and photograph of the holder, and often incorporating a chip and/or magnetic stripe for automated access to facilities; some of these are accepted at multiple sites, but mostly they are not interchangeable, so staff who regularly work at different sites have to carry several cards.

We have made significant progress towards introduction of a single trusted MOD credential, known as the Defence Multi-Application Smart Card (DMASC), for identification, physical access to MOD facilities, and electronic access to information services. A smart card is an essential component of the Defence PKI as it will be used to store PKI certificates. However, the DMASC rollout has been delayed indefinitely by the current financial situation. Unless this can be mitigated, cards with no personalisation will be issued to support initial use of the PKI service. This will reduce the level of assurance in the card as there would be a high risk of users sharing cards.

Provisioning / De-provisioning

The existing provisioning/de-provisioning capability involves manual processes that are slow, inefficient and prone to error. Some issues are:

- DII users cannot move seamlessly from the fixed to deployed environment, or between different deployments, without significant pre-planning, rigid scheduling and much manual effort, causing inconvenience and lack of flexibility.
- New staff cannot get a DII account quickly, resulting in expensive downtime for temporary staff hired at short notice.
- On DII, a user's access permissions cannot be revoked or changed rapidly and easily, with potential serious business and security impacts; changes cannot be made by the business.

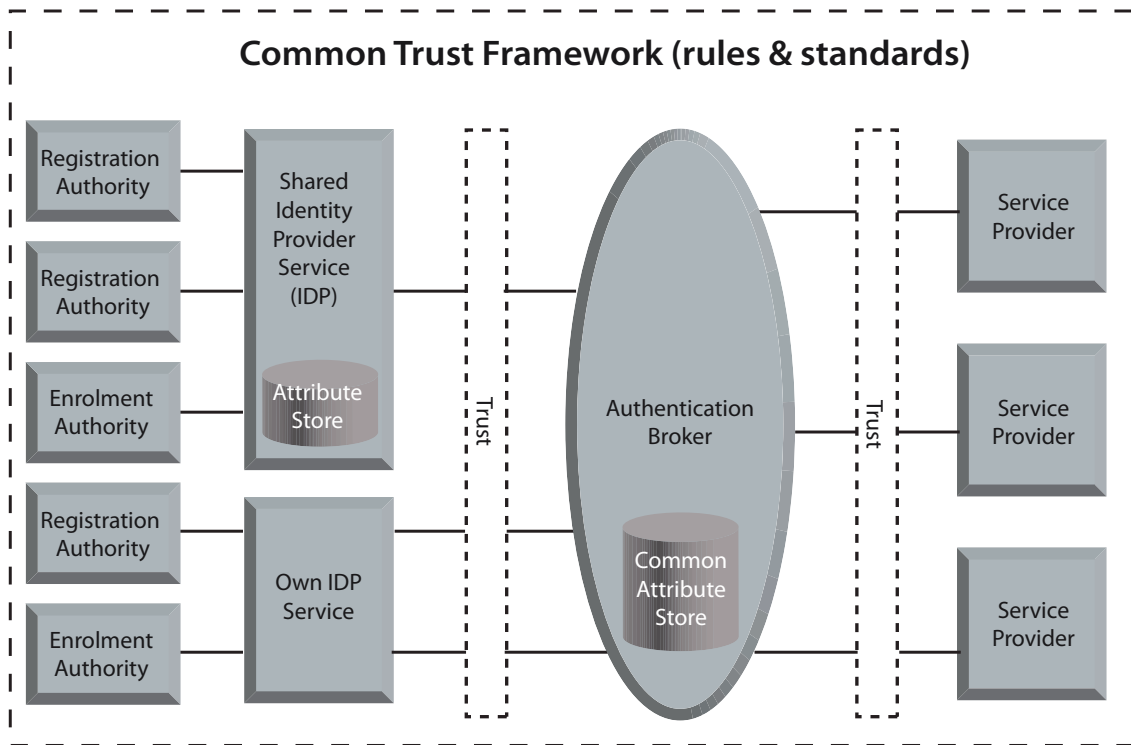
- Forgotten passwords require a manual reset by administrators, which is expensive and inefficient, and results in user downtime.

Logical Access Management

We have made some significant improvements in access management in the past few years:

- DII is providing a single joined-up information infrastructure which enables the majority of MOD people to access the information and services that they need to perform their jobs and conduct personal administration.

Figure 2 – EAS Trust Model



- MOD has worked with the Department for Work and Pensions (DWP) and the Department for Children, Schools and Families (DCSF) to develop the Employee Authentication Service (EAS), a shared service that provides public sector employees with access to Government applications from the Internet. The EAS solution is based on a Trust Model, illustrated in Figure 2, that incorporates a common Authentication Broker enabling multiple Identity Providers (each with its associated Registration and Enrolment Authorities) to provide authentication to multiple Service Providers. The EAS Authentication Broker and Trust Model have achieved CIO Council Champion Asset status, which means they must be used by Departments with similar requirements [7].
- The MOD Internet Access Shared Service (IASS) Initial Operating Capability (IOC) is providing 10,000 MOD employees with access to JPA and HRMS from the Internet via devices that redact sensitive personal data. IASS shares some components with EAS and includes some enhancements. These enhancements have been adopted as CTO Council Exemplar Pattern Services, which means they are recommended by the CTO Council for re-use by other Departments with similar requirements [8].
- We are working closely with the wider UK Government and external communities such as TSCP to develop common frameworks and standards for secure information sharing. TSCP has produced a specification for secure email over the Internet, and is developing one for document sharing through identity federation.

- We are implementing a Defence PKI and have ensured it will be interoperable with the PKIs of key partners.

There are many areas requiring further development:

- MOD applications and Shared Working Environments (SWEs) usually develop their own systems for managing users and controlling access, which is inefficient. It is inconvenient for users who have to log on separately to each application, and there could be security issues around management of multiple passwords.
- There are many SWEs across Defence based on stove-piped solutions that are not suitable for re-use.
- Gateways to MOD RESTRICTED and SECRET networks block encrypted email and there are no plans to address this. Further, it is likely that digital signatures will be stripped from email exiting or entering the DII domain.
- UK industry partners who are on the RLI have access to project-specific SWEs and limited information on the Defence Intranet. Other partners have no access to any internal MOD information or services.

Information Handling

We have recently developed an Information Handling Model (IHM) detailing how identities, permissions, information attributes and business rules are related to control information access [9]. It is based on the vision that information will be stored once on MOD Information Systems, with access to that single version controlled at that level, and access granted to authenticated users in compliance with policy and legislation. It outlines a number of principles, derived from extant policy, that must be implemented to achieve the vision. The key principle is that all information objects to which access must be controlled must be labelled at object level to enable Attribute Based Access Control (ABAC) decisions in accordance with policy. This means that identity permissions must correspond to information object attributes to allow access control decisions to be enforced technically. Information that does not require fine-grained control, which applies to most information on RESTRICTED systems, will continue to be handled as currently.

MOD capabilities at SECRET and below, including new DII software releases to be delivered during the next 18 months, will not be compliant with the IHM. Access to information held within core applications (e.g.; MOSS) will be controlled at the container level, such as team site or document library, and a user will have access to all or none of the information. This means some people will be denied access to information that should be available to them, while others will get inappropriate access. Also, as permissions are on the container, a removed item will lose those permissions. The future challenge is to enhance existing capabilities to implement the IHM.

Physical Access Management

A number of MOD establishments operate automated access control systems, but these are not networked so there is no efficient way of sharing visitor information between MOD establishments. Many establishments have no automated facility, resulting in a risk of unauthorised incursion by relying in visual identity checks, delays in processing visitors, and a potential health and safety issue caused by lack of records of who is on an establishment in the event of a fire or other emergency.

Until DMASC is delivered, we will continue to have many different types of MOD ID cards and site passes in circulation.

Federation

We have laid the foundations for federation with allies, industry partners and Other Government Departments (OGDs) through four groups. The current status is:

- Combined Communications-Electronics Board (CCEB) PKI Task Force, involving Australia, Canada, New Zealand, UK and US, is developing the architecture, processes, procedures, standards and technical activities to ensure interoperability of each National Defence PKI and achieve PKI cross-certification. Outputs include CCEB Publication 1010, a standard for cross-certification; each National Defence PKI can be cross-certified with each of the other National Defence PKIs by conducting a single policy mapping against Publication 1010. We have developed a draft PKI Cross-Certification Agreement (CCA) with the US DoD for SECRET and RESTRICTED.
- Transglobal Secure Collaboration Program (TSCP) is a cooperative forum of US/European Aerospace & Defence companies and government agencies working together to develop open-standards based specifications for PKI-enabled secure collaboration and assured information sharing. Certipath has established a PKI bridge for the Aerospace & Defence community. We have initiated the process to cross-certify with the Certipath bridge at RESTRICTED, enabling MOD to join a “web of trust” with other members of TSCP and the wider Defence community through a single cross-certification.
- UK Council for Electronic Business (UKCeB) Secure Information Sharing Community of Interest, established to promote secure information sharing and secure collaboration across UK Defence, and introduce capabilities that are appropriate for companies of all sizes in the end-to-end supply chain. This has identified priorities for UK Defence and is planning to conduct pilots for secure email and secure document sharing.
- Pan-Government Identity Management Working Group, established by the CTO Council, has developed a draft employee identity management strategy.
- Much work remains to be done to establish the required trusts, including audit of the Defence PKI to achieve tScheme approval, thus providing assurance to relying parties that the MOD trust service meets high quality standards.

Future IdAM Capability

The vision is to create a coherent and integrated IdAM capability as illustrated in Figure 1 by transforming the way that we manage and use identities and credentials to control access to resources. The required transformation is described in the next section.

Defence IdAM Transformation

Vision

A federated identity management capability that enables trusted access to, and secure sharing of, information by our people and partners across operational, support and business areas

Guiding Principles

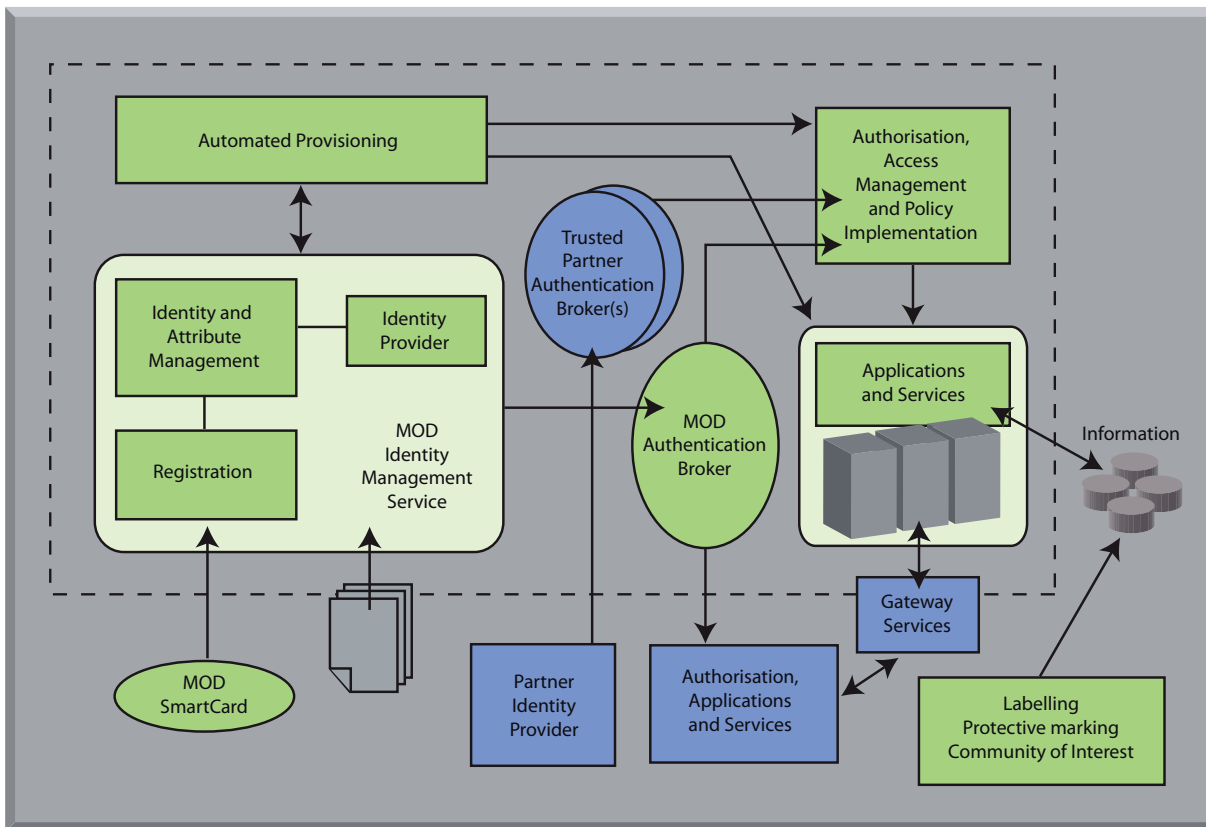
Delivery of the IdAM vision will be guided by the following principles:

- **One Individual, One Identity** – Each individual within MOD will have a single identity. The amount of data held on an individual will be sufficient to identify the person. Identity information will be stored once and shared with those who need it, including partners. There will be an authoritative source of identity information on MOD affiliates.
- **Life-Cycle Management** - Identity data, access privileges and business rules will be subject to rigorous life-cycle management. Each entity will have an owner/manager who will have facilities to manage its attributes, including the expiry date for access privileges.
- **Single Sign On (SSO)** – SSO will be implemented across DII so users log on once, using strong authentication, and have access to applications and services for which they have been approved without further log on. SSO will be implemented with Trusted Partners, enabling MOD people to log on to their MOD system and access external services, and external users to log on to their own system and access MOD services, without re-authentication.
- **Self-Service Tools** - Facilities will be provided to users and/or managers for re-setting passwords and requesting/activating changes.
- **Information Stored Once** - Information will be stored once on MOD Information Systems, with access to that single version controlled at the information object level and access granted to authenticated users in compliance with MOD policy and legislation.
- **Labelling** – Information that needs to be controlled (i.e.; for operational, business, security, commercial or legal reasons) will be labelled to support sharing. Interoperable labelling standards will be developed in consultation with partners; these will be underpinned by policy, procedures and ways of working concerning use of labels. Tools will be provided to facilitate labelling.
- **Identity Risk Management** – IdAM services will enable information sharing while safeguarded identity information.
- **Federation** – Services will be designed for federation. We will work with partners to develop common standards and specifications, for example through TSCP, and implement those standards across Defence.
- **Shared Services** – MOD will continue to contribute to delivery of secure and trusted IdAM services that provide Government employees and partners with access to cross-Government services.

MOD Trust Model

The Trust Model to be employed for delivery of IdAM services is illustrated in Figure 3.

Figure 3 – MOD Trust Model



This covers internal MOD capabilities (green) and external capabilities (blue). It applies to both SECRET and RESTRICTED. It provides for:

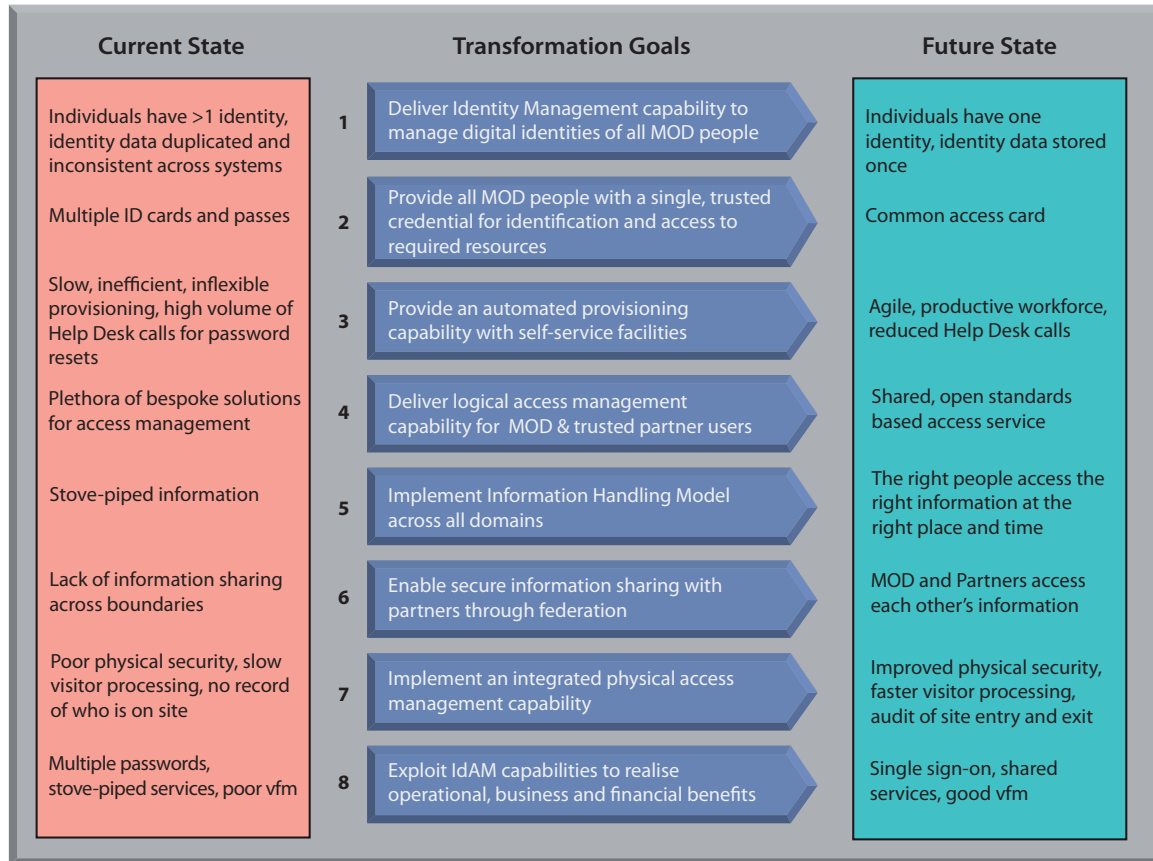
- Internal MOD users to access MOD applications and services for which they are approved using SSO.
- Internal MOD users to access external applications and services from their MOD system without re-authentication.
- External MOD and partner users to access appropriate MOD applications and services from the Internet, subject to policy, by authentication to the Government Gateway.
- Trusted Partner users to log on to their own systems and access appropriate MOD applications and services, subject to policy, without re-authentication.

It should be noted that the external interfaces shown in Figure 3 are purely illustrative; in practice, a number of federation models exist, some based on PKI and others employing non-PKI means of establishing trust, and they use a range of terms to describe the services provided, such as Federation Operator, Trust Broker and PKI Bridge. This strategy is solution agnostic and tries to avoid use of terms that convey a particular solution.

Achieving the Transformation

To achieve the Defence IdAM vision, we need to transform our business. This IdAM Strategy describes the required transformation in terms of eight goals. Figure 4 indicates how the eight goals will take us from where we are now to where we want to be.

Figure 4 – Defence IdAM Transformation



Annex B provides descriptions of the eight goals, together with their owners and the activities required to achieve them.

Benefits of the Transformation – Operational and Business

Delivery of the Defence IdAM vision will enable the following benefits:

- Easier collaboration and information sharing with partners by providing a common framework and standards for federated information sharing, including access to MOD information capabilities by trusted external users and access to external services by MOD users.
- Reduced information risk by employing stronger control of access to information, reducing the risk of inappropriate disclosure; improved protection of personal data by consolidating and securing identity data; automated provisioning / de-provisioning, enabling access permissions to be changed or revoked quickly and easily; strong two-factor authentication; workstations automatically locked when smart card removed; and wide use of encryption.

- More agile and productive workforce through MOD employees being able to access appropriate MOD information capabilities from non-MOD locations; rapid provisioning of new users or re-provisioning when users change roles; self-service provisioning when a user moves between fixed and deployed environments, or between different deployments; single sign-on to applications and services where appropriate; self-service password resets; and common ID card for physical access across MOD estate.
- Better management of identities and permissions including the capability to track the locations of deployed personnel; ability to ensure individuals with more than one MOD existence, such as a civil servant who is a reservist, have a single digital identity; and effective life-cycle management of the digital identities of all MOD people, including affiliates.
- Improved physical security by using the DMASC and an integrated MOD Access Control System for site/building access, thus placing less reliance on visual identity checks; enabling better control of who has access to an establishment through local management of electronic entry/exit permissions; permitting rapid changes to access permissions across the MOD if an individual is banned or a DMASC is lost/stolen; and providing an audit trail of establishment comings and goings, thus assisting evacuation procedures or supporting security investigations.
- Improved compliance with data protection and export controls by controlling access to information; and contributing to sustainable development by enabling MOD employees to access information from outside the MOD.

Costs and Financial Benefits of the Transformation

Annex C provides an overview of the benefits model [10] used to estimate the costs and financial benefits of the IdAM strategy. The total estimated costs and benefits are:

Cost / Benefit	£M
Initial Cost	33
Annual Cost	9
Annual Benefit	37

The costs and benefits are based on many assumptions and contain a high degree of uncertainty; further work is needed to reduce the uncertainty and take proper account of risk. However, the figures give a broad indication of costs versus benefits, and the scale of potential benefits is sufficient to make further work to deliver the strategy worthwhile. If all of the investment were to be made in Year 1, the full benefit would be realised in Year 2. The size of investment needed will preclude this in the current financial climate and, in any case, some goals will take longer to achieve; it is anticipated that the approach will be to deliver the IdAM capability incrementally, with priority given to delivery of quick wins and changes that realise the biggest benefits.

Delivery of the Strategy - Next Steps

Roadmap

The first step towards delivery of the IdAM strategy is to develop a roadmap. This will be carried out by CIO in close consultation with stakeholders, especially the proposed owners of the eight goals, and other key players such as personnel and security organisations. The approach will be to deliver the IdAM capability incrementally, with priority given to delivery of quick wins and changes that realise the biggest benefits. We will examine the feasibility of conducting one or more pilots to test solutions before commitment, especially in areas of biggest change such as implementation of the IHM. The target is to produce the roadmap in Q4 2010.

Maturity Model

An Identity Maturity Model is being developed for use by Departments to drive self improvement and assess maturity, but the way in which it will be applied and used is to be determined. MOD will consider its use when it becomes available.

Governance

Governance will be provided by the MODIS Executive Group, with lower level groups formed as needed.

References

1. MOD Information Strategy 2009, September 2009
2. MOD Information Assurance Strategy, September 2009
3. HM Government Safeguarding Identity, IPS Ref 295331, June 2009
4. Requirements for Secure Delivery of Online Public Services - Issue 1.0, July 2010
5. Government CTO Council Employee Identity Management Strategy, 2010
6. Transglobal Secure Collaboration Program Strategy 2009-2011 – see www.tscp.org
7. CIO Council Champion Case for Employee Authentication Service, sponsored by DCSF, DWP and MOD, December 2009
8. IASS Exemplar Pattern Capabilities, 2010
9. Defence Information Handling at RESTRICTED and SECRET, 2010
10. MOD Identity & Access Management Benefits Review, Detica DEA093D004-2.0, April 2010

ANNEX A - Definition of Terms

Access Management	Policies, procedures, standards and technologies to control access to logical and physical resources by authenticating credentials and authorising access to resources
Attribute	Information bound to a person or non-person entity that specifies characteristics of the entity such as role and privileges, or information about an information object that mediates access
Authentication	The process of verifying identity to confirm an entity is who he/she/it claims to be.
Authentication Broker / Trust Broker	Facilitates and simplifies secure information exchange by enabling multiple Identity Providers (with associated Registration Authorities) to provide authentication to multiple Service Providers.
Authorisation	The process of determining which activities are permitted by an authenticated entity based on permission/privileges of the entity and business rules associated with the activity
Credential	An attestation of identity, qualification, competence, or authority issued to an individual by a third party, such as a smart card or security token
Digital Identity (ID)	Electronic representation of a person or non-person entity (e.g.; device, application, service or process) comprising a unique identifier and set of attributes
Federation Operator (FO)	The FO provides governance and support for the federation, and has authority to create a framework in which identity assertions can be trusted and the privacy of identity information protected. Includes PKI Bridges, such as the TSCP Industry Bridge, and non-PKI Trust Brokers, such as the Government Gateway.
Identity Assurance	Relative measure of the strength of assurance that can be placed in an identity claim.
Identity Federation	The agreements, standards, and technologies that make identities and entitlements portable across autonomous boundaries, enabling authenticated users on one system to securely and seamlessly access information and services on another system without re-authentication
Identity Management (IdM)	Policies, procedures, standards and technologies for creating, maintaining, using and safeguarding personal identity information over its life-cycle
Provisioning / De-provisioning	Provisioning is the process of creating and modifying access privileges of identities. When automated provisioning is in place, user self-service can be implemented. De-provisioning is the process of revoking access privileges
Public Key Infrastructure (PKI)	The set of hardware, software, people, policies, and procedures to provide and manage X.509 certificates for public key cryptography. Certificates identify the individual named in the certificate, and bind that person to a public/private key pair. Certificates are used to provide data integrity, user identification and authentication, user non-repudiation, data confidentiality, encryption and digital signature services.
PKI Bridge	A hub between PKI organisations to facilitate and simplify use of PKI-enabled services between multiple organisations. If an organisation cross-certifies its PKI with a PKI bridge, it can use PKI-enabled services with any organisation trusted by the bridge through that single cross-certification. Examples include the US Federal Bridge and Certipath Aerospace & Defence Industry Bridge

PKI Cross-Certification	Establishment of a PKI trust relationship between two organisations via a Cross-Certification Agreement (CCA)
Self-Service Password Reset	Allows users to re-establish their own passwords, reducing help desk calls and back-office costs, by asking a set of questions to verify the user's identity
Single Sign-On (SSO)	Allows people who verify their identity on one system to carry their authenticated status over when accessing information services on another. The model works only among trusted partners
Smart Card	Card with embedded microprocessor used for identification and authentication.
Trusted Partners	Parties with mutual trust in each other's identity authentication through cross-certification or federation.
Two-Factor Authentication	Authentication based on something you know (e.g.; username and password) and something you have (e.g.; hardware token such as a smart card)
Unique Identifier	A digital identity comprises a unique identifier and set of attributes. The UK Government has adopted the National Insurance Number (NINo) as the Common Unique Identifier (CUI) for UK citizens, subject to further work on use of NINo. MOD has adopted the Person Unique Identifier (PUID), defined in JSP 329, to identify MOD people

ANNEX B - IdAM Transformation Goals

GOAL 1	Deliver identity management capability to manage the digital identities of all MOD people	Owner: D IS and D ISS
---------------	--------------------------------------------------------------------------------------------------	------------------------------

Goal 1 will deliver the policies, procedures, standards and technologies for managing the digital identities of all MOD people. The goal will be achieved by building on existing/planned capabilities, but current issues must be addressed. In particular, identity data must be sufficient to identify the person uniquely.

A digital identity will comprise a Person Unique Identifier (PUID) and set of attributes. The attributes will include:

- Data about the person, such as name, date of birth and nationality.
- A unique real-world identifier such as National Insurance Number (NINo), though an alternate to NINo will be needed for MOD people who do not have a NINo, such as exchange officers.
- The individual's civil service staff number, military service number and/or contract number.
- Details of the roles held, the access permissions associated with each role and the expiry dates of those permissions.
- The owner of the identity.

JPA and HRMS will continue to be the authoritative sources for identity information on military personnel and MOD civilian employees, respectively, but they must provide enough information to other MOD systems to identify the person uniquely. MOD will create an authoritative source of identity information on affiliates, such as contractors.

Individuals with concurrent existences in MOD, such as a civil servant or contractor who is also a military reserve, will have entries in JPA and either HRMS or the affiliates database; the IdM capability must cater for this to ensure the individual has a single digital identity with one PUID linked to both existences through the attributes. Individuals with serial existences, such as a person who serves in the armed forces then leaves and subsequently returns as a contractor, or a contractor who leaves then returns under a new contract, will already have a PUID, albeit inactive; the IdM capability must ensure the person is re-assigned the original PUID.

Each identity will have an owner who will have facilities to support identity life-cycle management, with automatic alerts when the expiry dates of access permissions are approaching.

The MOD IdM capability must be consistent with the emerging Government Employee IdM Strategy [5]. One of its key principles is that people working within Government will have a single identity, with identity information stored and maintained by the owning Department, and shared with Other Government Departments (OGDs) as required. MOD will need to develop policy and procedures to comply with this; it must address cases where: an employee of an OGD is a military reserve; a MOD affiliate works for an OGD and has primary allegiance to that OGD; and a MOD affiliate works for an OGD but has primary allegiance to MOD. For identities not owned by MOD, there must be a MOD proxy owner to manage MOD access permissions.

The IdM capability will deliver an Identity Provider (IdP) capability that provides a single trusted source of identity information for use across Defence and externally through federated interfaces with trusted partners. Data owned by MOD will be provided to OGDs as required to achieve the "one individual, one identity" principle.

The priority for this goal is to provide improved IdM of MOD people, but a longer term aim is to provide a capability for IdM of non-person entities (e.g.; devices, applications, services or processes).

This will enable access decisions to take account of machine identity as well as user identity. This will enable better and finer-grained security control on the access mechanisms protecting MOD data, allowing the right people in the right places to gain the right level of access to the right information.

Achievement of this goal will require changes across all lines of development, but the leading change will be provision of equipment capability, so the goal is owned by D IS and D ISS, supported by CIO for development of new policies and procedures.

GOAL 2	Provide all MOD people with a single, trusted credential for identification and access to required logical and physical resources	Owner: CIO
---------------	------------------------------------------------------------------------------------------------------------------------------------------	-------------------

The Defence Multi-Application Smart Card (DMASC) will be issued to all military personnel, MOD civilian employees and MOD affiliates to provide identification, physical access to MOD facilities, and electronic access to RESTRICTED information services. The DMASC design has been agreed by all major stakeholders including single services, civilian and service personnel branches and security organisations. It incorporates a contact chip, proximity chip, magnetic stripe, bar code, watermark and unique serial number; is personalised with photograph, service, military rank, name and expiry date; and is sealed with a special laminate featuring a MOD hologram. The card is tied to an individual by linking the card’s unique serial number to the individual’s PUID.

The DMASC will eventually replace all existing MOD ID cards and site/building passes. It is estimated that following completion of the rollout, some 370,000 individuals will hold active cards at any time; up to 100,000 reissues will be required per year to change details on the card, such as name or rank, and replace damaged, lost or stolen cards. It should be noted that an individual with two concurrent existences in MOD, such as a civil servant or contractor who is also a member of the armed forces, will have a separate card for each existence, but both cards will be linked to the same PUID.

Separate “white” cards will be issued for electronic access to SECRET and TOP SECRET systems. It is estimated that 50,000 active “white” cards will be needed at any time.

A Smart Card is an essential component of the Defence PKI as it will be used to store keys and certificates to support digital signing and encryption of electronic items. It is an enabler for delivery of this IdAM strategy as it will support two-factor authentication and single sign-on. MOD has opted for a combined ID card and Smart Card because the results of a pilot conducted in 2001, together with experience in organisations such as the US DoD, show that people take care of their smart cards when they are strongly linked to the individual (i.e.; personalised with name and photograph) and are needed to get into work.

Subject to business case approval, the Service Personnel and Veterans Agency (SPVA) will produce the DMASC, exploiting existing arrangements for production of military ID cards. SPVA has established the DMASC production line and is providing cards to the 10,000 users of the Internet Access Shared Service (IASS); these are identical to the DMASC but overprinted with “For IASS Use Only”. SPVA will use the IdM capability delivered under Goal 1 to tie an identity to a DMASC.

CIO will develop policy and high-level processes for issuing the DMASC during the initial rollout and steady state; this will be based on current methods and resources as far as possible, and include processes for dealing with lost, damaged, forgotten or expired cards.

This goal will affect all TLBs but is owned by CIO.

GOAL 3	Provide an automated provisioning capability with self-service facilities	Owner: D IS and D ISS
---------------	----------------------------------------------------------------------------------	------------------------------

Goal 3 will provide MOD with an automated provisioning/de-provisioning capability. Automated provisioning will enable MOD people to quickly, easily and efficiently obtain the information technology capabilities that they need when they need them. This will avoid the cost and risk of wide-spread provisioning of users “just in case” the capabilities are needed at some point in the future. It will enable better planning and execution of operations as staff move into and out of deployed locations, and avoid unproductive downtime when new people are hired or existing staff change roles.

Automated de-provisioning will ensure access permissions are revoked when their expiry date is reached (following a warning to the individual’s manager), overcoming the problem of individuals retaining access privileges to which they are no longer entitled. This will reduce security risk and cost. Automated de-provisioning will allow access permissions to be revoked rapidly across MOD if an individual is suspended or dismissed.

Self-Service provisioning will be enabled where appropriate. This will allow users, line managers or authorised demanders to request access to services or applications, and have changes implemented rapidly. This will include an authorisation check where appropriate. It will allow changes to access permissions to be made by line managers or authorised demanders, putting control of access to information in the hands of the business, where it belongs.

Self-service password resets will be enabled, keeping users productive and reducing the need for back office support.

Automated provisioning will utilise the DMASC and Identity Management capability to ensure the right users are provided with access to the right services and applications. It is a new capability for the MOD and will require changes across all lines of development. The main change will be provision of new equipment capability, so the goal is owned by D IS and D ISS, supported by CIO for development of new policies and procedures.

GOAL 4	Deliver a logical access management capability for MOD and trusted partner users	Owner: D IS and D ISS
---------------	-----------------------------------------------------------------------------------------	------------------------------

This goal will deliver the policies, procedures, standards and technologies to control access to logical resources by authenticating credentials and authorising access to resources. It will be achieved by building on existing/planned capabilities, such as the Defence PKI and IASS. The capability will have two components: an Authentication Broker and an Authorisation element.

The Authentication Broker will mediate between Identity Providers and Service Providers; it will accept an authentication request from a Service Provider and relay it to the appropriate Identity Provider, and accept the response from an Identity Provider and relay it to the appropriate Service Provider. In addition, the Authentication Broker will ensure that the Identity Provider conforms to the interface specifications and rules.

The Identity Provider and Service Provider could both be internal, or one could be external. For MOD and trusted partner users who are working outside the secure network, the Authentication Broker will ensure the correct verified identity information is passed to MOD Service Providers from external Identity Providers that it trusts through federation. This means that new Identity Providers and Service Providers can be added easily as each service only needs to establish two-way trust with the Authentication Broker, rather than having a separate trust and interconnect agreement with each Identity Provider. For MOD people working within the MOD secure environment, the Authentication Broker will provide appropriate identity and attribute information to external partner services that trust it.

The Authorisation element will enforce the Information Handling Model (IHM) (Goal 5). It will implement Attribute Based Access Control (ABAC) in accordance with policy. This means that the

permissions held by an entity requesting access must correspond to the information object attributes for access to be granted. The same policy based control will apply to internal and external users, but additional constraints will apply to external users, including MOD staff working outside the secure network and trusted partners. External users will have access to the same capabilities as internal users where appropriate, but the amount of functionality or information could be reduced. For example, IASS users can access HRMS and JPA from the Internet, but IASS redacts sensitive personal data to prevent unauthorised disclosure if the user is being overlooked.

The logical access management capability will support secure information sharing involving person-to-person (e.g.; email, web conferencing), person-to-application (e.g.; SWE, browser access to applications, access to Intranets) and application-to-application (e.g.; transfer of logistics data) exchanges. One of the highest priority requirements is for secure email over the Internet. This requires changes to mail and gateway services to allow digitally signed and encrypted email to be checked (without impacting the integrity of the original) and allowed to pass in and out of Defence networks.

Achievement of this goal will require changes across all lines of development, but the leading change will be provision of new equipment capability, so the goal is owned by D IS and D ISS, with support from CIO to develop new policies and procedures.

GOAL 5	Implement an Information Handling Model (IHM) across all domains	Owner: CIO
---------------	-------------------------------------------------------------------------	-------------------

This goal will implement the Information Handling Model (IHM) [9] to allow information to be stored once on MOD Information Systems, with access controlled at the information item level. This will involve:

- Developing interoperable labelling standards in consultation with partners.
- Agreeing information object attributes, with corresponding identity permissions, to achieve the required level of granularity to control access.
- Developing business rules to determine how access decisions are made in a variety of scenarios involving internal and external users, and internal and external information.
- Providing tools to support labelling.
- Implementing core capabilities that comply with the IHM.
- Developing new ways of working and embedding them across Defence.
- Developing and implementing policy for handling legacy data.

CIO will lead on delivery of this goal. The first step will be to gain agreement on labelling, attributes and business rules in consultation with allies, industry and OGDs. Then, the challenge will be to implement the required business change across Defence, including dealing with legacy data. CIO will work with stakeholders, including process owners, to ensure that implementation of the IHM enables users to perform their business functions without presenting unnecessary barriers.

GOAL 6	Enable secure information sharing with partners through federation	Owner: CIO
---------------	---------------------------------------------------------------------------	-------------------

Goal 6 will deliver the policy, procedures, standards, agreements and technologies to make identities and entitlements portable across autonomous boundaries, and allow authenticated users on one system to securely and seamlessly access information and services for which they are approved on another system without re-authentication.

This goal will be implemented by continuing to work closely with partners through the CCEB PKI Task

Force, TSCP, UKCeB Secure Information Sharing Community of Interest, and the CTO Council Identity Management Working Group. Future activities include:

- Cross-certifying the Defence PKI with the National Defence PKIs of CCEB members.
- Cross-certifying the Defence PKI with the Certipath Bridge, which will require the Defence PKI to undergo tScheme accreditation.
- Developing and implementing plans for cross-certifying with other members of the International Defence community, especially NATO.
- Exploiting IASS to enable wider access to MOD information services from the Internet.
- Developing and implementing plans for secure information sharing with OGDs including PKI-enabled sharing of medical information about military personnel with the NHS.

GOAL 7	Implement an integrated physical access management capability	Owner: D DBR
---------------	----------------------------------------------------------------------	---------------------

This goal, which is owned by DBR-DefSy, will deliver an integrated physical access control capability across all UK MOD establishments. This will provide:

- A central access control capability which will be linked to the IdM capability (Goal 1) to obtain details on all MOD people issued with DMASC (Goal 2), and hold information on all visitors to MoD establishments.
- A local access control capability at each MOD establishment linked to the ACR. This will serve as a local access control information repository; manage individual access permissions (linked to contactless card readers activated by DMASC); and produce temporary visitor passes.

GOAL 8	Exploit identity and access management capabilities to realise operational, business and financial benefits	Owner: CIO
---------------	--------------------------------------------------------------------------------------------------------------------	-------------------

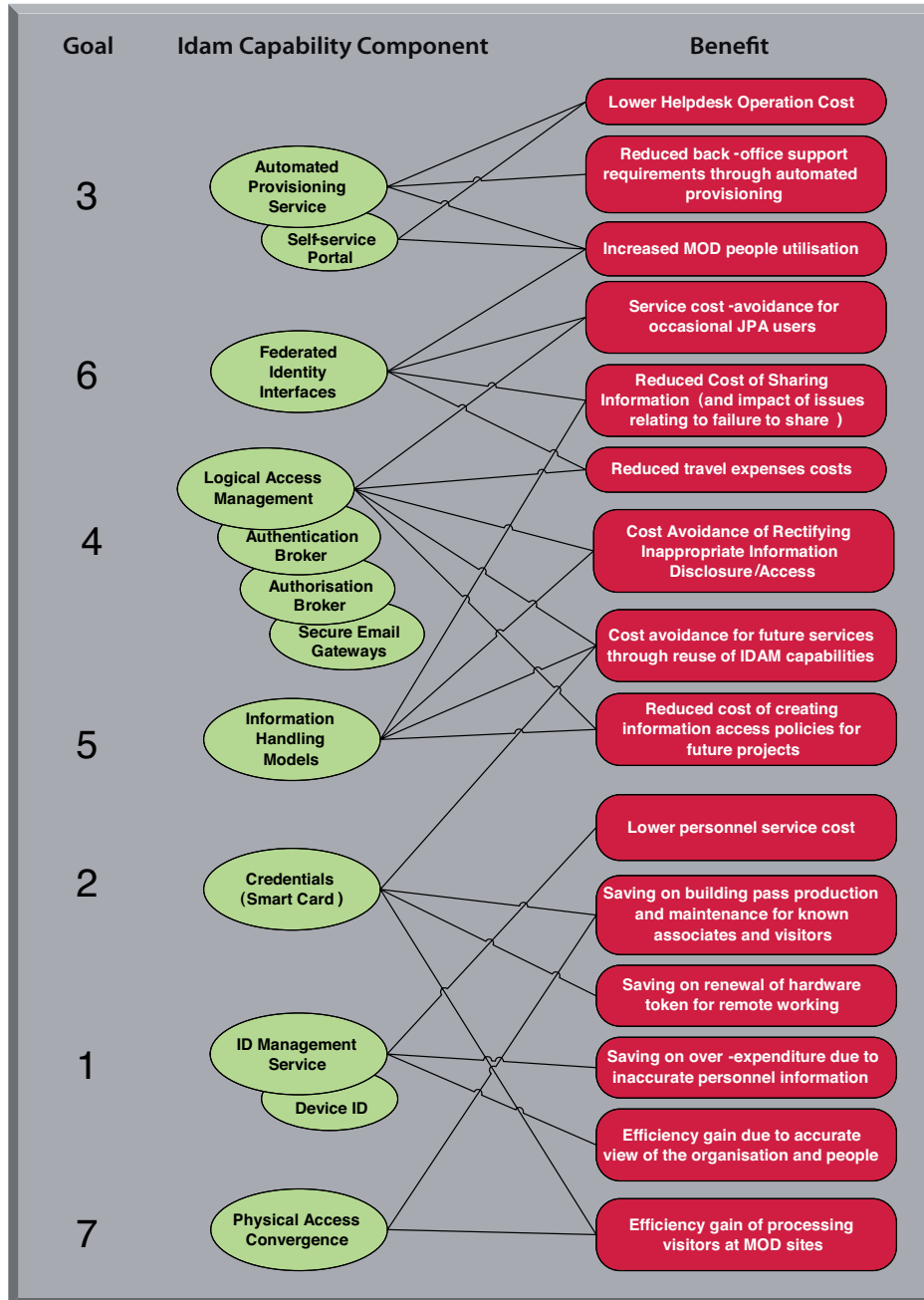
This goal, owned by CIO, will develop a plan for exploitation of the capabilities delivered in Goals 1 to 7, and oversee implementation of this plan. Planning work will:

- Identify programmes that could realise significant benefits by exploiting IdAM capabilities.
- Inform development of the IdAM roadmap so capabilities that enable the biggest benefits are delivered as early as possible.
- Identify programmes that can realise early benefits by exploiting existing/planned capabilities such as the Defence PKI.

ANNEX C

IdAM Benefits Review

A report was produced for CIO that reviews the potential benefits of the IdAM strategy [10]. It identifies fifteen financial benefits that could be enabled and includes a benefits map showing how the seven components of a federated IdAM capability relate to the fifteen financial benefits; this is reproduced below.



The report also presents the output from a benefits model showing the estimated costs of implementing and supporting the seven IdAM components, together with the estimated value of the benefits; this is reproduced on the next page. It should be noted that the costs and benefits are based on many assumptions and contain a high degree of uncertainty; further work is needed to reduce the uncertainty.

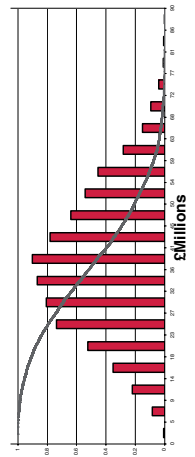
IdAM Benefits Model

MOD Identity and Access Management Strategy Benefits Model

This document has been produced for MOD CIO by Delica

Please note that the content in this table is automatically pulled across from the detailed tabs

Costs		
Solution Component	Initial Cost	Annual Cost
Identity Management (& Automated Provisioning) Service	£12,000,000	£3,000,000
Device Identity	£1,000,000	£300,000
Smart Card	£570,000	£1,900,000
Self-Service portal	£500,000	£100,000
Automated Provisioning Service (Included in IdM Service cost estimate)	£0	£0
Authentication Broker	£3,000,000	£600,000
Authorisation Broker	£2,000,000	£500,000
Secure Email Gateway	£3,000,000	£300,000
Information Handling Models	£5,000,000	£1,000,000
Federated Identity Interfaces	£1,000,000	£100,000
Physical Access Convergence	£5,000,000	£1,000,000
Total Cost Estimate:	£33,070,000	£8,800,000



Benefits		
Benefit Name	Logical Flow from Solution Component	Weighted Average
Cost Avoidance of Rectifying Inappropriate Information Disclosure/Access	Severe increases from use of labelled information with authentication/authorisation brokers and a single trusted credential requiring only one password to be remembered result in a lower chance of cost being incurred due to inappropriate information disclosure or access.	£1,000,000
Cost avoidance for future services through reuse of IDAM capabilities	Reuse of authentication and authorisation brokers in future MOD projects where IDAM is predicated will reduce cost of those projects.	£1,200,000
Reduced cost of creating information access policies for future projects	Implementation of the IHM means that much less effort must be expended on information handling policy for future projects.	£150,000
Reduced cost of sharing information with or providing services to external people	The federated identity interfaces allow trusted partners to use MOD services and for information to be shared without, for example, creating a new Shared Work Environment for each project. TSCP access - linear TSCP access + plus access to other partner services. Failure to share information gives rise to additional costs including major project schedule and cost risk.	£10,550,000
Reduced travel expenses cost	Federated identity interfaces and the authentication/authorisation brokers allow MOD people to access MOD information from non-MOD sites or partner information from MOD sites, reducing the need for physical travel.	£18,000,000
Increased MOD people utilisation	Less time is spent waiting for the helpdesk to affect password resets and provisioning, meaning staff are productive more of the time.	£4,250,000
Lower Helpdesk Operation Cost	Self-service portal provides many functions currently offered by the manned helpdesk, reducing the requirements (and so the cost) of the helpdesk. This benefit is particularly pertinent with regards to the self-service password reset functionality that will be offered by the self service portal.	£1,375,000
Reduced back-office support requirements through automated provisioning	Automated and business-focussed provisioning reduces the amount of provisioning being performed by the back-office support functions.	£8,199,000
Lower Personnel Service Cost	Improve provisioning business process -- Increasing efficiency. The identity management service enables lifecycle management and so reduces the number of unused accounts, directly reducing service costs.	£4,320,000
Saving on building pass production and maintenance for known associates as visitors	Adoption of the DMASC cards as physical access passes would remove the requirement for discrete building pass production for each different site.	£1,323,000
Saving on renewal of hardware token for remote working	Replacement of the current RSA physical tokens for remote working via DII with on-card authentication services that can be provided by DMASC.	£100,000
Saving on over-expenditure due to inaccurate personnel information	Example benefit chosen is supply of kit for military personnel. Reduction of cost of over or under ordering equipment and supplies for personnel.	£4,392,000
Efficiency gain due to accurate view of the organisation and people	Having a joined-up view of MOD people - including contractors - provided by the Identity Management Service, will allow projects such as e-Directory to realize significant benefits. More rapid and accurate response to FOI requests and PQs. Better MI to manage Defence business.	£36,475,000
Efficiency gain of processing visitors	Application of consistent physical access control enabled by the Smart Card (DMASC) solution component will allow physical access control processes to deal with true visitors and known MOD people differently, increasing the productivity of the latter.	£592,000
Service cost-avoidance for occasional JPA users	The extension of IASS to a wider audience will enable more MOD people to access key, but infrequently accessed applications such as JPA without requiring a DII account.	£10,800,000
Total Annual Benefits (Results of analysis run on 30 March 2010 - value at 50% confidence NOT EQUAL TO SUM OF AVERAGES):		£36,807,000

