HM Government

Safeguarding Identity

Contents

"I am delighted to support the publication of this strategy. At its core this strategy is about empowering people to use their identity information in ways which benefit them. Government has a clear role in enabling that process, and in ensuring that individuals' identity information is protected and subject to transparent and robust oversight. I fully endorse the actions set out in this strategy and look forward to supporting their delivery."

Alan Johnson
Home Secretary

"I welcome this strategy. In a global, digital age, the public sector needs to respond to rising public expectations. In the past, information was processed slowly and inefficiently, with mountains of paper being passed from place to place, increasing the potential for duplication, delay and error. To deliver world class public services Government must have a transparent and consistent approach to safeguarding identity information, including online services. This means agreed standards which ensure the highest level of protection for the most sensitive data. It also means being able to register your identity once and use it many times to access your services securely, in the confidence that you will only be asked for the minimum data and that your data will be safeguarded. This is key to improving delivery of public services and building public confidence."

Tessa Jowell
Minister of State, Cabinet Office

Foreword

Sir David Normington
Permanent Secretary, Home Office

James Hall
Chief Executive, Identity and Passport Service

The world around us is changing. People have much higher expectations of those who provide services to them. Technological advances make it possible for services to be delivered in ways we couldn't even imagine 10 years ago. People are more mobile and expect information and services to travel with them. In short, everyone expects the Government to deliver high-quality public services efficiently and conveniently, personalised to their needs wherever they are living.

Our ability to provide these services is dependent on our ability to know who everyone is, wherever and whenever they need a service. Today, an individual has to prove his or her identity to the Government in different ways for different purposes – and this variation creates vulnerabilities. In 2007 alone over 65,000 victims of identity fraud were identified and protected by the fraud prevention service CIFAS.[1]

While people understand that the Government needs to know who they are in order to provide them with the right services, people also rightly expect the Government to look after their personal information and protect it in an open and transparent way.

The Government and its agencies, as well as the rest of the public and private sector, already collect a lot of information about citizens. One option is to allow the current variation in systems and processes to continue. But that would not provide the improvements in convenient services or safeguards that the public rightly expect.

The aim of this strategy is to make it easier for citizens to prove and safeguard their identity, building on the foundation provided by the Data Protection Act 1998 and the Cabinet Office Review of Data Handling Procedures in Government. In future, everyone should expect to be able to:

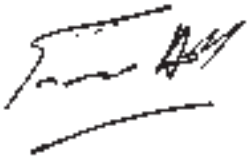
- register their identity once and use it many times to make access to public services safe, easy and convenient;
- know that public services will only ask them for the minimum necessary information and will do whatever is necessary to keep their identity information safe;
- see the personal identity information held about them – and correct it if it is wrong;
- give informed consent to public services using their personal identity information to provide services tailored to their needs; and
- know that there is effective oversight of how their personal identity information is used.

[1] www.cifas.org.uk/default.asp?edit_id=561-56

Government will seek to meet these expectations with this strategy which has three key strands:

1. The agreement of common building blocks for identity – definitions, standards and credentials – which will increasingly be used in systems and processes across Government;
2. The agreement of some specific improvements in the way public services are delivered, such as a common approach to assuring identity when providing services online; and
3. The agreement of a consistent approach to the necessary safeguards to protect everyone's personal identity information, in line with the data protection principles and the Cabinet Office Data Handling Review.

This strategy is being published by the Home Office, which leads on identity issues, through its agency the Identity and Passport Service on behalf of the Government. It marks an important step forward in underlining the Government's commitment to safeguard people's identity. We look forward to continuing to work with the cross-Government Safeguarding Identity Strategy Group to deliver the important next steps which this strategy outlines.



1. Introduction

1.1. This strategy is the agreed result of extensive cross-Government work. Recognising that the Government only uses individuals' identity information on behalf of the public, this strategy sets out the actions the Government will take to improve how it uses identity information. The principal audience for this document is the Government and its delivery partners who will need to implement the strategy. This strategy addresses important and sometimes contentious issues. The Government is committed to being as transparent as possible in developing work in this area, which is why this strategy will also be available to the public.

1.2. In Chapter 2, we set out the **case for change** – identifying **service improvement** and **public protection** as the key drivers.

1.3. Chapter 3 outlines **our strategy** – describing the key **building blocks** and the **public service improvements** that will be delivered.

1.4. Chapter 3 also describes the **safeguards** which will be put in place to ensure that personal identity information is held securely and the way it is handled is open and transparent.

1.5. Chapter 4 recognises the **wider context** of this work – and acknowledges the importance of continued engagement and collaboration with colleagues in **local Government, the devolved administrations, the third sector and internationally.**

1.6. Chapter 5 describes the specific identity requirements of the **business** community and confirms the Government's commitment to ensuring that benefits are delivered both for individuals and for business.

1.7. Chapter 6 sets out the **next steps** in taking this strategy forward. It describes the **governance** arrangements that will be used to ensure it maintains momentum and the **timetable for delivery**, including when individuals will be able to see the improved outcomes that this strategy identifies.

2. The case for change

2.1. Across Government, systems and processes for handling information about people's identity have evolved over time. Considerable progress has already been made in improving the way information is used and this is delivering benefits in terms of both public protection and making people's lives easier.

2.2. Examples of those benefits include the following.

- **Government departments and other public sector organisations are making an increasing number of services available online.** For example, Directgov (the official UK Government website for citizens) received 11 million visits per month between September and November 2008. A number of financial transactions are also due to converge on to Directgov during 2009 (including self-assessment tax returns, Child Benefit applications and the student tax checker).
- **Individuals can choose to have their personal identity information shared in ways that increase convenience and reduce processing times.** For example, an individual applying for a driving licence from the Driver and Vehicle Licensing Agency (DVLA) now has the option to share the digital photograph and signature from their passport so that they do not have to provide this information again.
- **Advances in the use of forensic technology are helping bring more offenders to justice.** For example, the use of mobile fingerprint devices by police forces to search against the National Fingerprint Database allows for quicker identification or verification of a subject's identity.
- **Identity cards for foreign nationals from November 2008 are making it easier for them to prove who they are and their entitlement to work and access services while in the UK.** In addition, the introduction of the cards has led to a number of successful prosecutions for offences such as attempting to extend leave to stay in the UK by deception.

2.3. Information about an individual's identity has at the same time become a valuable commodity because of what it can make possible. That is why people try to use it for criminal or fraudulent purposes. Both the Government and the private sector have a clear responsibility to ensure that, in enabling the positive benefits of identity information to be realised, the risks from fraud and crime are properly mitigated.

Cost of identity fraud

It is estimated that identity fraud costs the UK economy £1.2 billion per year and accounts for a criminal cash flow of £10 million per day. The impact this has on individual victims of identity theft varies. It can take up to 48 hours' work for a typical victim to put their affairs back in order and clear their name. In cases where a 'total hijack' has occurred, it may take the victim over 200 hours and cost up to £8,000 before things are back to normal.

Sources: www.identitytheft.org.uk/cms/assets/cost_of_identity_fraud_to_the_uk_economy_2006-07.pdf
www.cifas.org.uk/default.asp?edit_id=561-56

2.4. The evolution of systems and processes has created variation in the identity information that is collected and in how that information is used and handled across the public, private and third sectors.

2.5. While in many cases this is both necessary and reasonable, variation has also created both inconvenience and vulnerabilities for the citizen.

- People still need to prove their identity in different ways when accessing different parts of the public sector, and face many requests for the same basic information but often in a slightly different format.
- People are often asked to provide more information than is strictly required to facilitate a particular transaction (for example, address details).

- It is difficult for individuals to see what identity information is held about them, or to update this information if their circumstances change.
- People are not yet able to receive consistently from Government the same level of personalised services that they have come to expect from the private sector.
- Government services do not always have confidence in each other's processes – leading to duplication and lack of trust.
- Duplication and inconsistency decrease efficiency and deliver poor value for money for taxpayers.
- People's identity information is coming under increasing threat from those who wish to use it for fraudulent or criminal intent, facilitated by the growing availability of such information and expanding technological capability.

Identity credentials

Ninety per cent of the adult population has an identity credential.

The most common credentials reported as being used are:

- passports – 63%;
- driving licences – 57%;
- birth certificates – 32%; and
- household bills or phone bills – 27%.

A range of other documents or cards are sometimes presented – such as NHS cards – which are usually relevant only in the areas in which they are issued.

Source: Proof of Identity Research by TNS Consumer, April 2008

2.6. If we can put this right, we will deliver to the citizen over time a better service, better protection for their information and better value. The following chapters outline how this might be achieved – how the Government will build on the improvements already under way and seek to deliver a simple, common approach to safeguarding and using identity.

3. Strategy

3.1. We have a simple aim. We want everyone who interacts with Government to be able to establish and use their identity in ways which protect them and make their lives easier. Our strategy seeks to deliver five fundamental benefits. In future, everyone should expect to be able to:

- register their identity once and use it many times to make access to public services safe, easy and convenient;
- know that public services will only ask them for the minimum necessary information and will do whatever is necessary to keep their identity information safe;
- see the personal identity information held about them – and correct it if it is wrong;
- give informed consent to public services using their personal identity information to provide services tailored to their needs; and
- know that there is effective oversight of how their personal identity information is used.

3.2. Government will meet these expectations with this strategy which has three key strands:

- the agreement of common identity 'building blocks' – definitions, standards and credentials – which will increasingly be used in systems and processes across Government;
- the agreement of some specific improvements in the way public services are delivered, such as a common approach to assuring identity when providing services online; and
- the agreement of a consistent approach to the necessary safeguards to protect everyone's personal identity information in line with the data protection principles and the Cabinet Office Data Handling Review.

Building blocks

3.3. We set out below how we propose to achieve convergence in three critical areas.

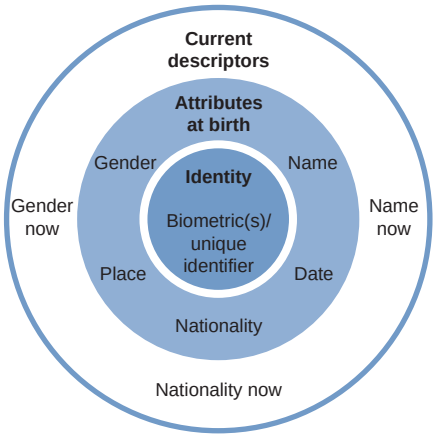
i) Common definition of identity

3.4. Identifiers are the pieces of information with which people establish and use their identity; names, signatures, passwords, usernames, PIN numbers and fingerprints are all examples of identifiers.

3.5. Today, the information an individual uses to prove they are who they say they are has at its core a person's name and address. This is information that can and does change, sometimes quite frequently. This makes it difficult for public services to have confidence that they are dealing with the right person – and it creates a burden on individuals to prove that they are who they say they are, often in the form of relatively insecure documents such as utility bills. In the future, the information used to prove an individual's identity will be centred on aspects which do not change.

3.6. Our intention is that, at the core of the information used to prove identity will be biometrics, such as photographs and fingerprints. These are characteristics which can be held securely and linked to other information by way of a unique identifier. The unique identifier will not be printed on a document or card, making it more secure. This small amount of reliable information about an individual will form the 'minimum identity data set'. The next layer will consist of information established at birth which does not change, such as name at birth and nationality at birth. The next layer will reflect changes since birth – that is, information true now, such as current name and nationality. These layers are illustrated in Figure 1.

Figure 1: Identity and identifiers: layering identity information



3.7. Further information about an individual which is relevant only within a specific context can be held separately – linked through the unique identifier. For example, personal health details or information about an individual's benefits or taxes should continue to be held separately. An individual can access this information through the existing identifiers that are already known to them (for example, NHS number, National Insurance number).

3.8. This layered approach delivers benefits.

- An individual's core identity is based on information – both biometric and biographic – which does not change. This is more reliable.
- When accessing services, individuals should need to provide only a small amount of information to prove that they are who they say they are. In some situations, an individual may only need to use their fingerprint (avoiding the need to provide information such as their address).
- Personal information which is not part of an individual's identity (such as details related to health or to benefits) is held separately and does not form any part of their identity information.

3.9. It is proposed that, over time, the Identity and Passport Service (IPS) will hold the minimum identity data set. This would make it possible for other Government departments to share this information with the knowledge or consent of the individual. For individuals, this means greater confidence that less information about them is being held across Government, and that what is being held is secure. For public services, it means less time spent establishing and updating identity information (for example, change of address) that is secondary to their core business.

3.10. It will take time to move from today's ways of proving identity (name and address) to the new model, but the Government will start working now by looking at the most secure and convenient ways of identifying people and rationalising the large number of identifiers which are currently used.

Action 1: Minimum identity data set definition

The information individuals use to establish and prove their identity should be based on an agreed minimum set of trusted data. Individuals should be able to use that information to access a range of services.

Steered by the Identity Management Standards Policy Group (IMSPG), IPS together with the Department for Work and Pensions (DWP) and the Driver and Vehicle Licensing Agency (DVLA) will lead development of the minimum set of trusted identity data.

Milestone: The content of the minimum identity data set to be agreed by the Safeguarding Identity Strategy Group (SISG) by the end of the first quarter (Q1) of 2010.

Action 2: Converging on the new definition of identity

Together, Government departments should move towards a common definition of identity based on the minimum identity data set.

IPS together with DWP and DVLA will develop an approach and road map for migration towards the new definition of identity based on the minimum information set.

Milestone: The approach for moving to a new definition of identity to be agreed across Government by end Q2 2010.

ii) Common standards of identity

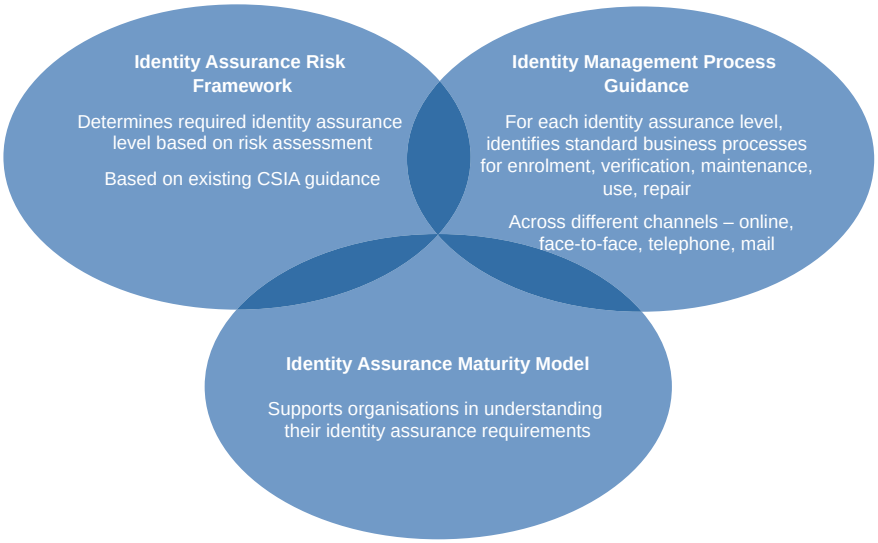
3.11. Identity standards define the common business and technology processes which an individual or an organisation uses to establish or prove identity.

3.12. Agreeing a common set of standards can deliver real benefits. Standards ensure that individuals can prove their identity when accessing public services in a simple, convenient and consistent way. They also help individuals to have confidence that their information is being looked after properly and proportionately. A common set of standards will help organisations to establish their own requirements and provide a clearer means of answering questions such as: What information do we need? How much of it do we need? How do we ensure we handle it securely and appropriately?

3.13. For this to be achieved, the Government will provide clear and accessible guidance: the Safeguarding Identity Framework. This will offer for the first time a single framework of authoritative identity standards for UK public services. Development of the framework will be facilitated by the cross-Government IMSPG.

3.14. The framework is made up of three components set out in Figure 2.

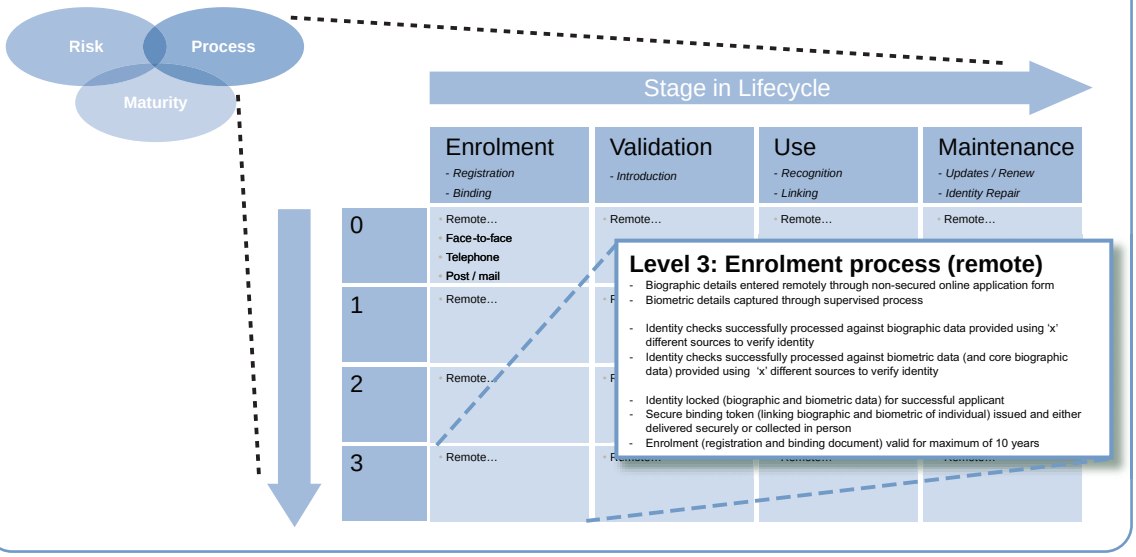
Figure 2: Safeguarding Identity Framework: the three core components



3.15. **Identity Assurance Risk Framework:** this will allow organisations to determine what their requirements are for handling identity information. It will use a structured risk assessment approach to ensure that information is being properly and proportionately managed. It will also help organisations to comply with relevant policy and guidance including that relating to information assurance.

3.16. **Identity Management Process Guidance:** for processes such as enrolment, validation, maintenance, use and repair, this guidance will help public services establish the appropriate level of integrity and security for a particular process or transaction. In Figure 3, the example of enrolment is used to show how this process might be delivered remotely with a high degree of assurance.

Figure 3: Safeguarding Identity Framework: Identity Management Process Guidance



3.17. **Identity Assurance Maturity Model:** this will help the same public services to assess their current performance against a clear set of measures. Over time, this will help to drive self-improvement and will allow Government to better understand how different organisations are performing.

Action 3: Safeguarding Identity Framework

Across Government, identity information should be dealt with in a standardised way – reducing duplication, speeding up processing times and improving efficiency.

IPS will lead development of the *Safeguarding Identity Framework* – setting out a single authoritative framework for how Government will use, store and share identity information, and how it will monitor its ability to do so.

Milestone: First version of Safeguarding Identity Framework approved and released by IMSPG across central Government departments by end Q1 2010.

iii) Common set of credentials

3.18. Credentials are the means by which individuals prove their identity. Passports, driving licences, birth certificates, utility bills, credit cards, passwords – these are all examples of identity credentials.

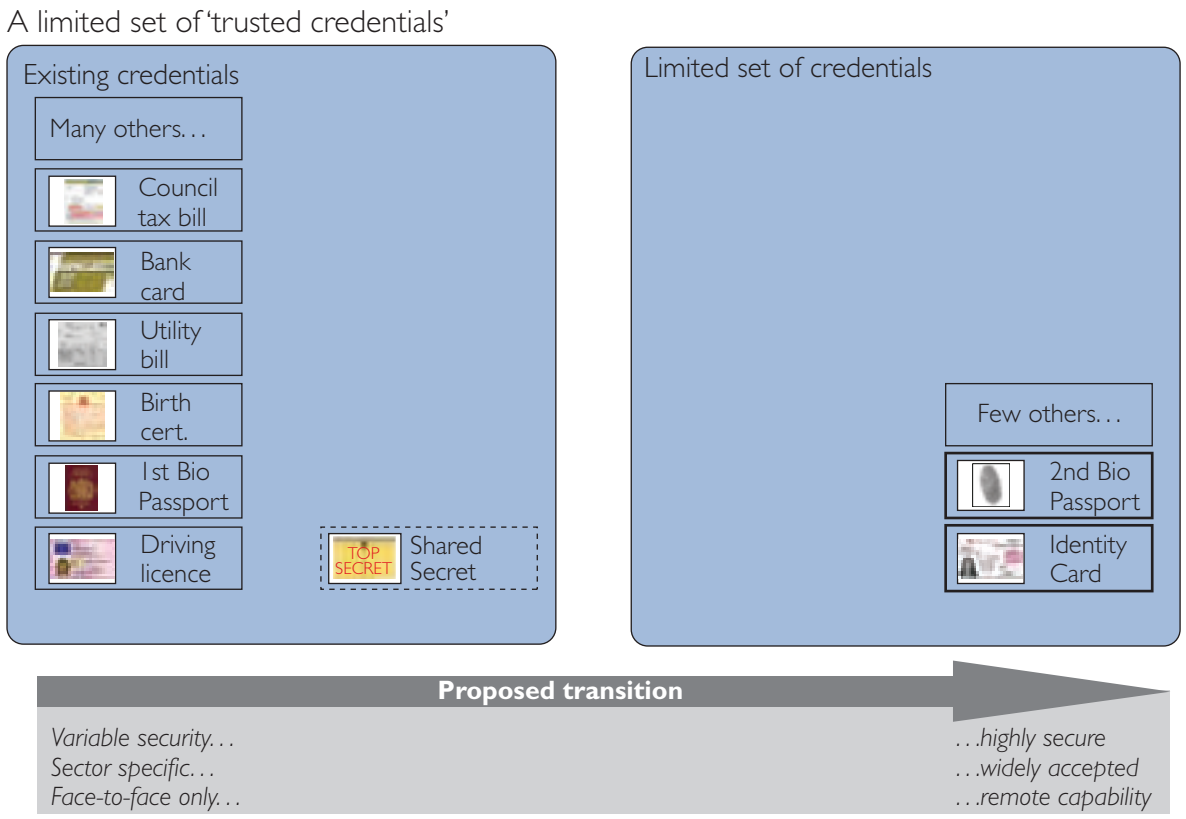
3.19. In recent years, the importance of these credentials has increased dramatically. More and more transactions require proof of identity and are increasingly conducted remotely (by phone or online). However, the credentials themselves vary in their degree of integrity and their multiplicity makes usage unnecessarily complex both for the customer and for the service provider.

3.20. Moving to a limited set of trusted credentials will be a key part of the Government's service transformation. For customers, it will provide a secure and straightforward route to establish identity. For public services, dealing with a smaller number of credentials with common features will reduce complexity and cost, and enable the shift to more cost-effective interactions with their customers, such as online.

3.21. In the first stages of this strategy, public services will continue to use the credentials that are already available. However, the Government will clarify the level of integrity provided by each of today's existing credentials so that the service provider can make good decisions about which credentials should be accepted in a particular situation.

3.22. As the National Identity Service (NIS) is introduced, new credentials will be developed that offer greater levels of security and confidence. Biometric passports and identity cards, due to be introduced in 2012, will form the foundation of a future smaller trusted set. As these NIS credentials become more widespread, the need to use existing non-NIS credentials is expected to diminish.

Figure 4: Identity credentials



Already happening...

Registering for the first time with a GP practice

Rod has recently arrived from the USA to study in England. He has authority to stay and wants to register with a GP, so he goes to a local practice and asks to be registered. The practice has an open list of patients and the receptionist asks Rod if he has previously been registered with a GP, so they can trace his previous medical records. Rod says he has not, and is then able to use his identity card to confirm his immigration status. He is living within the practice area so he is accepted and his details sent to the local primary care trust.

Action 4: Defining a trusted set of credentials

Trusted credentials should allow individuals to prove who they are, make it easier for Government to verify identity, and protect people by making it hard to use them in a fraudulent way.

Steered by the IMSPG, IPS will lead the development of the trusted set of credentials – building on biometric passports and identity cards.

Milestone: The trusted set of credentials to be defined and agreed by the SISG for cross-Government consensus by end Q4 2009.

Action 5: Converging to a trusted set of credentials

In time there will be convergence from the broader range of existing identity credentials to a smaller, trusted set.

IPS will lead the development of a clear plan for assisting organisations to converge with the trusted set of credentials – in line with their business needs.

Milestone: Cross-Government plan for convergence on trusted credentials to be agreed by end Q1 2010.

Public service delivery improvements

3.23. Using the building blocks, a number of business and technology changes can be delivered which will transform the way identity is used across Government. This will support and complement the delivery of world-class public services as envisaged in *Excellence and Fairness*[2] and *Working Together: Public Services on Your Side*.[3]

Remote access to public services

3.24. Central to the transformation of the delivery of public services, as set out in *Excellence and Fairness*, is people's ability to access those services conveniently. Individuals should have the option to use a 'single door to Government' to access a range of personalised services and information to which they are entitled. Methods of access will include online, telephone and kiosk services. Using a single, reliable and secure system for remote access will allow individuals and organisations to establish and verify identity quickly.

3.25. For example, many services are currently provided through the Directgov portal, but different User IDs and passwords are required to access different services. The aim is that, in future, people will have just one.

Action 6: Shared remote access service definition

Individuals should have the option to use a 'single door to Government' to securely access a range of services.

IPS and DWP will together develop a shared remote access service based on existing Government assets including the Government Gateway.

Milestone: Operating model and business case for shared remote access service to be agreed by SISG by end Q3 2009.

Action 7: Converging to a shared remote access service

In time, all public sector services will migrate to a single access authentication service. Departments will want to make this transition when it is right for their business and when there are clear benefits to their customers from doing so.

IPS, DWP and Her Majesty's Revenue and Customs (HMRC) will work with departments to help them identify the optimum time for transition and develop a road map setting out how convergence will be achieved.

Milestone: Road map for convergence on remote access solution to be agreed by SISG by end Q1 2010.

[2] *Excellence and fairness: Achieving world class public services*, Cabinet Office, 2008

[3] *Working together – Public services on your side*, HM Government, 2009

From 2010…

Owning and using identity to make life easier

Grace has just turned 21 and is starting to apply for jobs in the design sector. In addition to the GCSEs she achieved at school, she has completed several different strands of learning and further education since the age of 16, including a part-time university course and some vocational training at a design institute. Using her unique learner number Grace can access her educational records and can choose to give prospective employers access to the relevant elements. Grace can now easily and conveniently provide a clear and accurate picture of her background and accredited qualifications.

Public sector employees and access to information

3.26. The public expects the Government to handle personal information carefully and securely. This includes making sure that:

- public sector employees are who they say they are and appropriate background checks have been completed prior to employment; and
- public sector employees have access only to the information that they need to carry out their role.

3.27. An integrated approach to pre-employment checking will ensure that the process for completing required biographical, security, right-to-work, criminal and other checks is appropriate, efficient and effective. The process will take account of security requirements, experience of applicants and employers and the strategic objectives of Government departments and their delivery agencies.

Action 8: Employment checking

The Home Office will work with other departments to recommend an integrated approach to pre-employment checking.

Milestone: Proposal and implementation actions for an integrated approach to pre-employment checking service across Government to be agreed by the SISG by end Q2 2010.

3.28. Employee authentication will provide a consistent, secure and robust system for ensuring that access to identity information is properly controlled. Information will be restricted to those trusted employees who need to see or verify that information in order to carry out a particular transaction. Only the necessary personal information is disclosed on each occasion depending on the nature of that particular transaction.

Action 9: Controlled employee access to information

IPS will work with departments to recommend a 'best of breed' model, which departments can apply to their systems, in order to ensure that access to the minimum necessary identity information is restricted to trusted employees who need it to carry out a particular transaction.

Milestone: Model for restricting employee access to identity information agreed by Q3 2010.

National Identity Service

3.29. The NIS will deliver the means to prove identity quickly and effectively, and provide a secure and straightforward way to safeguard personal identities from misuse. The NIS will securely 'lock' a person's biographic information to their unique facial and fingerprint biometrics on a National Identity Register (NIR).

3.30. From 2009, the first identity cards will be issued to British citizens, with their biometrics stored in a chip on the card as well as on the NIR. From 2012, anyone applying for or renewing a passport in the UK will also enrol their fingerprint biometrics on the NIR and will be able to choose whether they want a biometric passport, an identity card or both.

3.31. The NIS is already a reality for those foreign nationals who have been issued with an identity card since November 2008, improving protection at the border and detection of crime. By November 2009, 75,000 foreign nationals will have a card, using it to prove their right to stay in this country legally.

3.32. The vision for the NIS is that it will become an essential part of everyday life; underpinning interactions and transactions between individuals, public services and businesses and supporting people to protect their identity. The NIS will do this primarily through further 'identity services': the processes and tools with which people can prove or check identity.

By 2012...

Proving identity quickly and easily

Clare works for a multinational retailer and has to travel a lot for work. She used to carry her passport around with her all the time but it became dog-eared and messy. Now she keeps her identity card in her purse and only uses her passport when she is going outside Europe.

When she arrives back at Manchester airport, Clare walks straight up to an automated gate. She enters the gate, puts her identity card in a slot, puts her index finger on a scanner and the other side of the gate opens to allow her through.

Further identity services

3.33. IPS is leading the development of an identity services strategy. This will set strategic requirements for value-added identity services, and a road map for agreeing how such services can be delivered. The strategy will develop broad categories of identity service which will always be operated with the consent of the individual, and are likely to include, among others:

- **'Know your employee'** services to enable employers to verify that a job applicant is who they say they are, or that they are entitled to work in the UK for instance; and
- **'Know your customer'** services, to enable commercial and public sector partners to verify a customer's identity, for example before a mortgage is issued or an age-restricted product sold; such services also have the potential to enable businesses to improve their processes and reduce the cost of compliance with Government regulations.

By 2012...

Confirming the right to work

Bill is the owner of a coffee shop and has just made a job offer to Sally to start work next week. Before she can start, it is standard practice to check her identity and right to work so Bill asks Sally for evidence of both. Sally chooses to show Bill her identity card which confirms both her identity and her right to work in the UK and gives consent for him to get her National Insurance number from the IPS. Bill is pleased by this as it means he can get her payment and deductions set up quickly and correctly first time.

3.34. The experience of other countries suggests that identity services need to be developed gradually, over time, with new functionality being added as the number of people enrolled grows and the appropriate technology develops further. It also shows that access to public sector services often comes first, but in the end it is both public and private sector applications that will drive utility.

3.35. Identity services should never be at odds with the safeguards put in place to protect the privacy of the individual, or the integrity and security of the NIR. Part of the wider strategy will be to articulate the fundamental integrity and security principles within which the development of identity services must take place.

Action 10: Identity services

IPS will lead the development of an identity services strategy which will set out the strategic requirements for identity services and a road map for agreeing how the services could be delivered.

Milestone: Identity services strategy and road map to be agreed by end Q4 2009.

By 2012...

Reducing complexity and linking services

Sheena has just given birth to her second child. When her first child was born, she found that although she could register the birth while she was still in hospital, she had to do a number of things for which she needed a birth certificate: apply for Child Benefit, claim Child Tax Credit and organise who would open the account for the Child Trust Fund.

This time, Sheena reads about a notification service in her local hospital and looks online to see if it can help. She is pleased to find that after she registers the birth, she needs to provide only one set of information – Government then does the rest for her. Sheena and her new baby are now registered for all they are entitled to. In addition Sheena receives an email offering her more information about support available from the local Sure Start Children's Centre.

By 2012...

Using identity conveniently and easily

John arrives for his first day at university and reports for registration. On arriving at the main office he sees two queues for registration. The first queue is for people who have an identity card, enabling them to quickly and conveniently establish their identity and complete the registration process. The second queue is for anyone who does not have a card, requiring them to use various paper-based forms of identity to complete the same registration process, which takes more time. John is really pleased he registered for his card as he is able to join the first queue and complete the process quickly and easily.

Safeguards

3.36. The rights of individuals in respect of sharing personal information are set out in legislation; in common law; and in the European Union Data Protection Directive1995. In the UK, the Data Protection Act 1998 and the Human Rights Act 1998 in particular provide robust protection for personal information and for individuals' right to privacy.

3.37. Public trust and confidence in Government relies on strong accountability and oversight. It is Parliament, and the Commissioners it appoints, that provide the top-down safeguards for personal information and privacy.

3.38. The Commissioners play a vital role in ensuring that individuals' rights are protected. The powers of the Information Commissioner are being enhanced, providing the ability to apply financial penalties where there is a reckless and wilful breach of the data protection principles. To ensure the new NIS is also open and transparent, a new Identity Commissioner is being appointed with a clear role to protect individuals' rights and to hold Government to account.

3.39. When the Government shares personal identity information for reasons of national security, countering terrorism and tackling crime and fraud, legislation will be in place to define what Government can do. That legislation provides clear safeguards including limiting the organisations to which information can be provided without consent, and the limited circumstances under which such sharing will be permitted. Ensuring that the rights of individuals are protected in these cases, and providing oversight for Government action, is the responsibility of the Intelligence Services Commissioner and the Surveillance Commissioner who are appointed to focus specifically on this area of information use.

3.40. The aim of this strategy is to empower individuals to establish and use their identity in ways which protect them and make their lives easier.

- see the personal identity information held about them;
- correct that information if it is wrong;
- know how personal identity information held about them is used; and
- know that there is effective oversight of their personal identity information.

Identity ownership: access, maintenance and repair

3.41. Identity information changes as people's circumstances change – when they move home, when they get married, when they change job and so on. **Identity maintenance** is the process by which people can update their information.

By 2012…

Accessing and maintaining identity information

Sarah has just moved house and goes online to find out what she needs to do to change her address details on the NIR. She discovers she can update these details online, and starts by verifying her identity using her identity card. As no additional documentation is required, she updates her address details using the online form and receives an email confirming that her address details have been changed.

3.42. If information is recorded inaccurately, or if it has been compromised, it needs to be repaired. **Identity repair** is the process by which information that has been subject either to error or fraud is corrected and the consequences of the inaccuracy are addressed. While responsibility for maintenance rests with the individual whose circumstances have changed, responsibility for identity repair usually rests with the service provider, and wherever possible identity repair processes will be coordinated across Government.

Action 11: Identity ownership: access, maintenance and repair

Individuals should be able to see their identity information and easily update it if it is wrong.

IPS will develop and coordinate a common approach to the maintenance and repair of an individual's identity information, providing clarity on the role of the individual, of IPS (particularly with regard to the NIR) and of other Government departments.

Milestone: Initial proposals for a common approach to identity maintenance and repair to be agreed by SISG by end Q4 2009.

Action 12: Identity ownership: convergence

To help improve the experience of the individual, organisations should ensure that simple processes are in place for maintaining or repairing information which they hold and which is not currently shared across Government.

IPS will coordinate the convergence of current identity maintenance or repair processes to common standards.

Milestone: Progress update to SISG on convergence of identity maintenance and repair processes by end Q2 2010.

Transparency in the use of personal identity information

3.43. Government already shares some personal information about individuals in order to provide effective and efficient services. In many cases public authorities will have an individual's consent to share information, but, in order for this to work both effectively and transparently public services and individuals need to understand when and how to both ask for, and give, informed consent to the use of their identity information so that this can be done consistently across Government.

Action 13: Linking services by consent

Individuals should be able to share their personal identity information across Government services when they choose to do so – with their informed consent.

IPS, the Ministry of Justice, DWP, HMRC and the Information Commissioner's Office will together develop a consent model for sharing identity information across Government. MoJ plans to consult on the sharing of personal data by public authorities shortly and the outcomes of the consultation will shape any model that is developed.

Milestone: Consent model for sharing identity information across Government to be agreed by SISG by end Q3 2010.

4. Recognising the wider context

4.1. This strategy sets out the Government's plans for future improvements in how identity information is used and handled. The actions set out in this strategy will only deliver those improvements if they receive the support and endorsement of a wide range of stakeholders and partners.

4.2. Across the UK Government, devolved administrations, local Government, European and international partners and the third sector, there will be complex issues to resolve concerning the specific identity information needs and issues that exist.

4.3. Together with the Department for Communities and Local Government, IPS will work with the Local Government Delivery Council and the Local Chief Information Officer Council to establish how best to engage with local authorities to ensure they are able to help inform and shape the Government's identity strategy.

4.4. IPS will also work with the Devolved Administrations, in recognition that many areas of service delivery are devolved, to ensure they are able to inform and shape the Government's identity strategy.

4.5. Over time the expectation is that Government organisations – both central and local – will converge with the common approach this strategy sets out. Each organisation will need to determine for itself how far and how soon they are able to converge.

4.6. The focus of this strategy – and the actions it contains – is to provide a framework within which those decisions can be taken: in time reducing variation and improving the service offered to citizens.

5. Business identity

5.1. This strategy focuses on improving the way in which the Government safeguards the identity of individuals. The other major group of customers that interacts with Government is businesses. Businesses need to establish and use their identity, and in many respects the fundamental requirements for business identity are the same as those for individuals. The principles and recommendations set out in this strategy provide a firm foundation for further developments in business identity management.

5.2. Current systems and processes for safeguarding business identity have evolved over time and have resulted in a degree of variation that both creates vulnerabilities and reduces efficiency.

5.3. Business interactions with Government cost time and money both for the businesses themselves and for Government – around £20 billion according to a recent National Audit Office report.[4] Whilst much of this is the cost of proper and necessary regulatory compliance – such as providing tax returns and complying with employment law – improved business identity management has the potential to enhance the simplicity and efficiency of interactions between Government and business – reducing costs and freeing up resources.

5.4. By 2011 businesslink.gov.uk will become the online information and transactional channel for businesses with central Government. Through using businesslink.gov.uk, businesses will be able to increase efficiency and reduce the time and cost of interacting with Government. Burdens will be further reduced if businesses can identify themselves and provide the necessary information only once.

5.5. Government will also make it easier for businesses to access support services. These have previously been provided by a range of central and local Government bodies. Businesses have had to apply to each body separately – which is inefficient for both the business and the body providing the support service. The Business Support Simplification Programme is reducing the number of support products to around 30 and exploring ways of simplifying the process of application.

5.6. In addition to the developments in this strategy, there are three key areas in which more work is required to address the specific additional needs of businesses:

- enabling individuals to establish their authority to act on behalf of a business;
- establishing the separate identity of all types of businesses, including sole traders and partnerships; and
- developing the minimum data set for business identity, building on the minimum data set for individuals but adding other necessary specific elements such as business location.

Action 14: Business identity strategy

The specific identity information needs of businesses (and those individuals who represent them) need to be properly considered across Government.

HMRC and the Department for Business, Innovation and Skills will lead work across Government to develop a complementary identity strategy addressing the requirements of the business sector. They will also help to ensure that the needs of business are fully considered in other actions set out in this strategy.

Milestone: Complementary identity strategy developed for the business sector by end Q3 2009.

[4] *The Administrative Burdens Reduction Programme 2008*, National Audit Office

6. Next steps

Governance

6.1. The Identity Management Strategy Group (IDMSG), chaired by Sir David Normington (Permanent Secretary, Home Office), has provided cross-Government oversight to shape the development of this strategy. During its development, the strategy has been regularly reviewed with ministers through the Home Secretary's Identity Cards Working Group.

6.2. As this strategy is implemented, the Government will maintain a focus both on delivering the actions it sets out and continuing to develop the strategic narrative and road map for this work.

Safeguarding Identity Strategy Group

6.3. To mark the shift from strategy to delivery, IDMSG will be re-focused as the Safeguarding Identity Strategy Group (SISG). This group will continue to own and develop the strategic narrative and road map for safeguarding identity. It will use a benefits framework as a way of maintaining focus on the aims of the strategy, regularly discussing:

- cross-Government priorities where alignment with the strategy provides opportunities or challenges;
- areas of potential benefit not yet being realised which could influence the direction of cross-Government initiatives;
- realisation of the benefits of the strategy and the potential to broaden those benefits to other areas of Government; and
- opportunities to refresh the strategy to meet continued needs across Government.

6.4. This group will continue to be chaired by the Permanent Secretary of the Home Office and will have senior-level membership from those departments with a strong interest in or dependency on identity issues.

6.5. Development of the strategy has been aided by working with key sectors across Government. IPS will continue to facilitate and support work within these sectors.

Identity Management Standards Policy Group

6.6. SISG will continue to be supported by the IMSPG, chaired by the Executive Director, Integrity and Security, IPS. This group's principal aims are to:

- promote shared understanding of identity management standards across the public, private and third sectors;
- bring together existing identity management standards initiatives in the public sector and foster the development of new standards (such as the Safeguarding Identity Framework) where required; and
- provide a first point of contact for identity management practitioners seeking advice on standards and best practice.

6.7. As the new standards framework develops, we propose to build in parallel an approach to their governance which will facilitate their adoption as quickly as possible.

Delivery

6.8. The Public Sector Reform Group, supported by the Chief Information Officer (CIO) and Chief Technology Officer (CTO) councils, continues to provide cross-Government oversight of delivery of the Service Transformation agenda of which Safeguarding Identity Framework is a critical component. The CIO and CTO Councils have a particularly important role to play in approving the Identity Standards Framework and supporting the champion assets delivered to support this strategy.

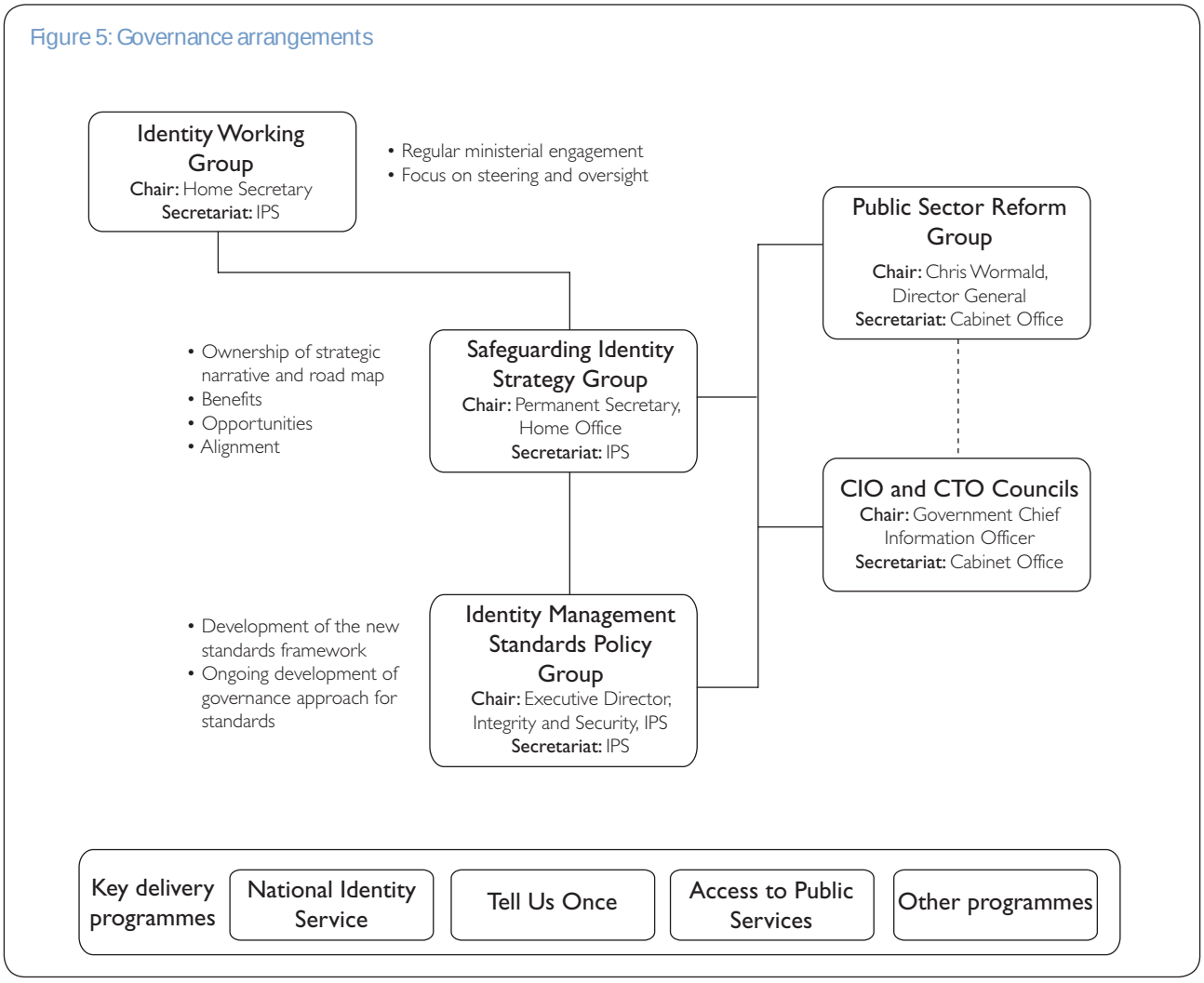
6.9. Parts of the Safeguarding Identity Strategy are being delivered through existing cross-Government programmes such as the NIS, Tell Us Once, the Employee Authentication Service and new programmes such as Access to Public Services, which is a feasibility study that IPS and DWP are working together to mobilise.

6.10. The SISG will recognise and, in many cases, help to shape the benefits delivered through these programmes. It will support and reinforce, not replicate, the appropriate governance structures already in place to manage delivery of these programmes.

Legislative requirements

6.11. All the proposals in the Safeguarding Identity Strategy will need to take full account of existing legislative requirements and constraints. This includes the legislation that governs the delivery of individual public services as well as any wider statutory duties, such as those arising from the Data Protection Act or the Human Rights Act. In addition, where new ways of sharing data are to be proposed, then the need for changes to existing legislation may also need to be considered.

Figure 5: Governance arrangements



Action 15: Steering the strategy

To deliver the benefits of Safeguarding Identity: Making Services More Effective, it is essential that work is properly coordinated across Government.

IPS will maintain the lead role in coordinating and supporting the oversight and governance model.

Milestone: New governance arrangements to be functioning by end Q2 2009.

Timetable for delivery

6.12. The detailed timetable for completion of the 15 actions is set out in Figure 6. However, the outcomes to be delivered will be as follows.

6.13. From now until 2012, the Government will focus on improving current arrangements and building the foundation for future improvements through:

- delivering and embedding the building blocks identified in this strategy – including agreeing the minimum data set, producing the Safeguarding Identity Framework and establishing the trusted set of credentials;
- delivering the early stages of the NIS – building on the Critical Workers Identity Card and rolling out identity cards to early interest groups and young people;
- utilising new technology to improve services and safeguard identity – making educational records available online, enabling individuals to view and track benefits applications online, and delivering increased use of biometric checks at the border and for front-line police officers; and
- putting in place the right oversight and governance structures to ensure benefits are delivered beyond 2012.

6.14. Between 2012 and 2015, the Government will focus on building on the strong foundations that will be in place including:

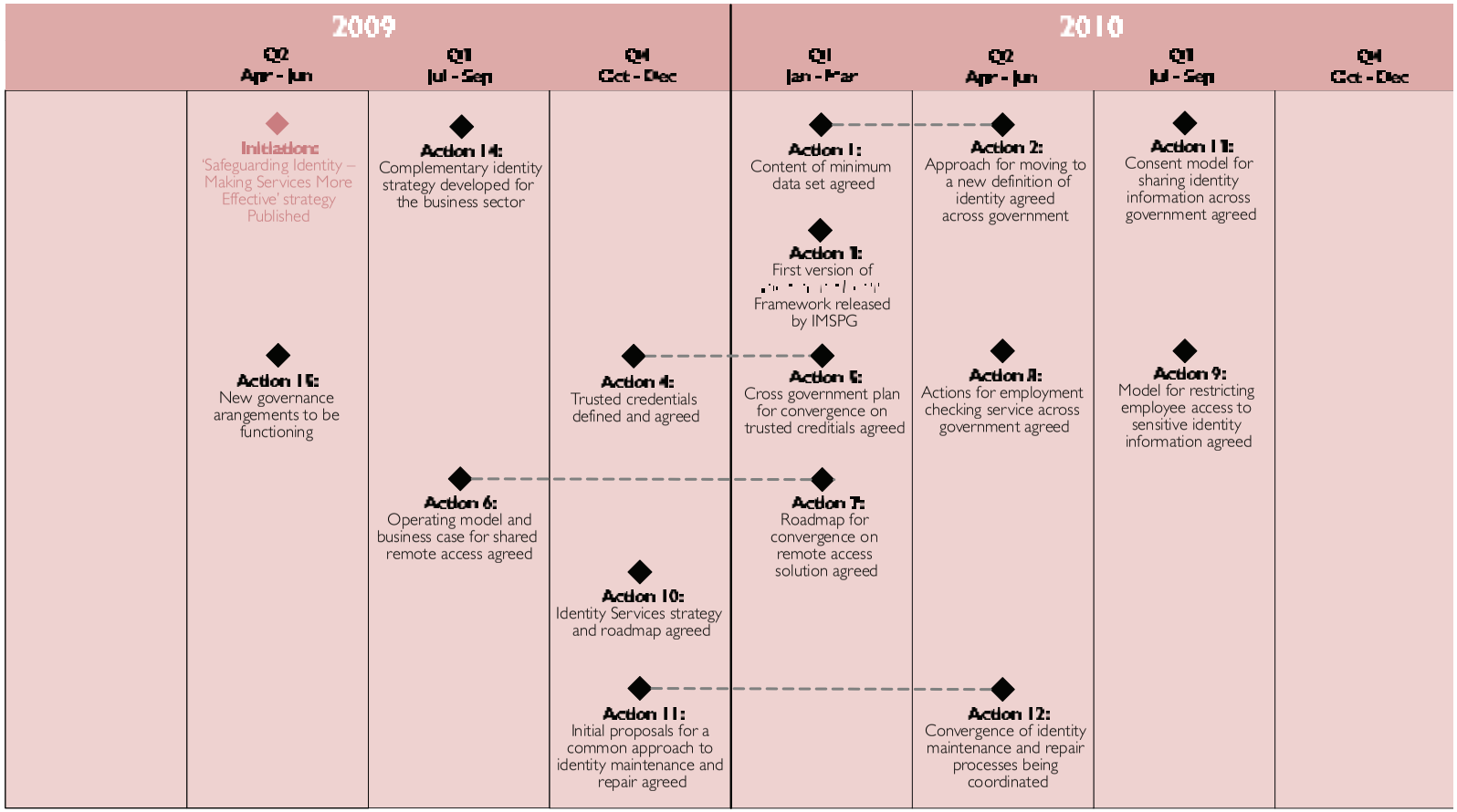
- converging existing systems and processes with the common standards set out in the Safeguarding Identity Framework – ensuring individuals have a consistent and high-quality experience across Government departments;
- reducing the number of credentials – and increasingly relying upon the trusted set – to establish and use identity;
- delivering the full NIS – with second biometric passports and identity cards available to all applicants; and
- ensuring people are able to easily access services remotely – building on the success of Directgov and expanding the range of services that can be accessed online.

6.15. Beyond 2015 there should be a period of further radical change in the use of identity information, facilitated by improvements in technology. This period will be focused on improving services in the public and private sectors. Those changes will happen rapidly and be hard to predict, but if the broad aims of this strategy are achieved strong foundations will be in place. In particular:

- across Government, individuals' identity information will be handled consistently and appropriately – with greater clarity for individuals and organisations;
- a common definition of identity will be accepted across Government – based on simple and secure information, in many cases using biometrics;
- the new NIR will be commonly used across Government as a single, convenient and secure system for establishing and using identity; and
- highly secure biometric-enabled credentials will be routinely and widely used – either second biometric passports or identity cards (with people able to choose either, both or none).

6.16. This strategy marks a significant step forward in tackling existing vulnerabilities and ensuring that the Government delivers improvements both now and in the future.

Figure 6: Actions timetable



Produced by the Identity and Passport Service. Ref: 295331. June 2009.