

Identity and authentication



Self-service relies on trust between the customer and the provider. Confidence about the identity of the person at the other end of an electronic transaction is critical to developing trust in the system. Ever since the days of local e-government in the early 2000s, having a secure process for identity and authentication has been the holy grail for establishing long-term trust. As providers of social care information, advice and services, local authorities are planning for an upsurge in online demand, stimulated by the 2014 Care Act.

What steps should your local authority take for handling user identities for online social care?

Contents

Why important	03
Basic concepts	04
Important stakeholders	06
Local government practice	08
Options for local solutions	13
Conclusions	18

ACKNOWLEDGEMENTS

ADASS, LGA and Socitm would like to thank the following people and organisations for their contributions:

Sue Dawes

Open Identity Exchange

Rebecca Hales

Government Digital Service

Ian Litton

Warwickshire County Council

Phil Stradling

NHS England

LEAD AUTHOR

Martin Greenwood

Socitm

EDITOR

Richard Pantlin

ADASS

1. WHY IMPORTANT

THE DIGITAL WORLD

Identity and authentication were hot issues in ICT circles over ten years ago, yet councils are still building the topic into their latest strategies, clearly marking it up on their 'to do' lists for the next three to five years.

The world has changed greatly, making this a more pressing issue than ever. The quotation opposite from a report in 2004 is just as valid in today's digital world.

Most people now own smartphones, tablets and other portable digital devices. As a result, digital access to information and services is now widespread amongst most parts of the population. Their expectations of instant results have increased exponentially.

This revolution clearly changes the working lives of all those who deliver local public services. Mobile, flexible and home working are all very much part of today's working life, especially for those like social workers who work away from the office.

These trends all shape public policy, nowhere more so than in health and social care. Providing care for unprecedented numbers of older people, often without family support and subject to long-term, incapacitating health conditions, is a rapidly escalating challenge. The Government has put in place a legislative framework in England to meet this challenge with the Health and Social Care Act 2012 and the Care Act 2014.

Rising demand will create unsustainable costs. Austerity is driving channel shift, as evidenced by the mandating of online interaction for the new universal credit scheme.

Theoretically, technology also makes it easier to share up-to-date information across agencies, making it more possible to integrate health and social care.



The clock is ticking towards the 2005 deadline for councils to deliver their services electronically. For many of these services, the council will want to 'authenticate' the person who is requesting the electronic transaction – or in other words, be confident that they know who they are. The authentication scene is complex, and changing fast. Understandably, councils are confused about which direction to take, and worried about the impending deadlines.



Source: Knock, knock: who's there?: an overview of authentication for electronic service delivery (Socitm Insight, November 2004)

NEED FOR ASSURANCE

In this digital world, both the public and the organisations that serve them need to be able to trust electronic transactions.

Authentication is key to developing trust, especially for more complex transactions.

When we board an aeroplane, we trust that we will arrive safely at our destination. We know that we cannot be 100% certain that will be the case because we know that accidents occur, but we have sufficient confidence to make the trip. The odds look favourable. Similarly, we cannot have complete faith in whatever authentication method we employ, but the chances of failure or identity fraud have to be low enough for us to trust the system.

In the world of adult social care, many types of transaction require the same degree of trust, including:

- delivering direct payments or services
- sharing personal and confidential information
- obtaining entitlement and eligibility information from other organisations.

Identity and authentication in this world are very much at an early stage of development. The rest of this briefing provides an overview of current developments, starting with a reminder of some basic concepts and important stakeholders.

2. BASIC CONCEPTS

PRINCIPLES OF IDENTITY ASSURANCE

The Privacy and Consumer Advisory Group (PCAG) has published the identity assurance principles to inform and guide the privacy aspects of identity-related initiatives within government, and in particular the GOV.UK Verify programme.

CLASSES OF RISK

As a first step we should consider the types of potential risk. There are four classes of risk to online public services:

- **Financial** transactions where there is potential for fraud and/or financial loss
- **Confidential** transactions involving personal or commercially sensitive data where there is potential for data protection breaches and fines from the Information Commissioner's Office (ICO)
- **Regulatory** situations where there is a need for a robust audit trail
- Situations that might involve risk to the **organisation's reputation**, should they be mismanaged or poorly administered.

LEVELS OF ASSURANCE

Transactions require differing levels of trust. If the user wants to download a form or access a policy statement, there is no need to know who is making the request. However, if the user wants a financial benefit, then the provider needs much greater assurance. There are four levels of assurance (LOA):

- **LOA1**, when a relying party needs to know that it is the same user returning to the service but does not need to know who that user is
- **LOA2**, when a relying party needs to know on the balance of probabilities who the user is and that the user is a real person
- **LOA3**, when a relying party needs to know beyond reasonable doubt who the user is and that the user is a real person
- **LOA4**, same as LOA3, but with a biometric profile captured at the point of registration.

Source: <https://www.gov.uk/service-manual/identity-assurance>

PRINCIPLE	CONTROL AFFORDED TO INDIVIDUAL
1 User control	Identity assurance activities can only take place if I consent or approve them.
2 Transparency	Identity assurance can only take place in ways I understand and when I am fully informed.
3 Multiplicity	I can use and choose as many different identifiers or identity providers as I want to.
4 Data minimisation	My request or transaction only uses the minimum data that is necessary to meet my needs.
5 Data quality	I choose when to update my records.
6 Service user access and portability	I have to be provided with copies of all of my data on request; I can move/remove my data whenever I want.
7 Governance/certification	I can have confidence in any identity assurance system because all the participants have to be accredited.
8 Problem resolution	If there is a problem I know there is an independent arbiter who can find a solution.
9 Exceptional circumstances	Any exception has to be approved by Parliament and is subject to independent scrutiny.






Table 1 Nine principles of identity assurance (PCAG)

MODELS OF AUTHENTICATION

Authentication is about the verification of a piece of data. Identity assurance seeks to establish a person's identity to a level commensurate with the risks incurred, should it be wrong.

Broadly speaking, there are five models of authentication:

- face-to-face/manual (eg paper certificates, passports)
- user name and password-based systems
- single sign-on systems (eg re-using social media identity)
- multi-factor systems (ie using more than one method of authentication from independent categories of credentials)
- identity provider-based (IdP) systems (ie providing data for verifying who users say they are)

MODEL	LEVEL OF ASSURANCE	COST TO ORGANISATION	COST TO INDIVIDUALS	SET-UP COSTS
 Face-to-face	HIGH	HIGH	HIGH	MODERATE
 User-id/ passwords	LOW	LOW	HIGH	LOW
 Single sign-on	LOW	LOW	LOW	LOW
 Multi-factor	HIGH	MODERATE	MODERATE	HIGH
 Identity provider	HIGH	LOW	LOW	HIGH

Legend: **BENEFITS** **DRAWBACKS**

Source: IDX Economics of Identity White Paper

ATTRIBUTE EXCHANGE

Authenticating identities is important, but with explicit and clear consent of the individual providing proof of attributes that people claim for themselves, such as how long they have lived at an address or what they earn, can add extra layers of assurance to make a bigger difference in transforming services. Attribute exchange enables people to prove online that they are, for example, registered disabled or in receipt of specific benefits. It facilitates much more sophisticated online transactions by establishing trust frameworks between service providers and attribute providers that will effectively eliminate paper proofs from complex transactions (eg using passport data and a photograph for provisional driving licence).

It is defined by OIX 'the **online, real-time** exchange of data **specific to the transaction in hand**, with the **verified user present** and with their **full knowledge and permission**'.

Online and real-time: this meets the requirement for digital by default, giving the user the opportunity to complete transactions online and in real time.

Specific to the transaction in hand: this meets the data minimisation principle embedded in the Data Protection Act by ensuring that only the data required for the transaction is exchanged. This in turn builds user trust and acceptance.

Verified user present: the user, whose identity has been verified to Level of Assurance 2 (LOA2), is present during the transaction and can assist the process if required. For example, to provide additional information that might assist user account or record matching with either the relying party or the attribute provider.

User's full knowledge and permission: with the user online and present in the transaction, explicit permission can be sought to share their data. Crucially, this avoids the need for complex data sharing agreements between organisations that can take years to negotiate. Users who do not wish to give permission can be offered alternative means to obtain the service based on traditional channels.

Source: *Towards an architecture for a digital blue badge service* (Open Identity Exchange, August 2015)

3. IMPORTANT STAKEHOLDERS

OPEN IDENTITY EXCHANGE (OIX)

The OIX was formed in 2010 following a request by the new Obama administration in the USA to establish how it might use open identity technologies to allow the American public to more easily, efficiently, and safely interact with federal websites.

It develops and registers what it termed trust frameworks. These are pre-negotiated sets of business, legal, and technical agreements that provide mutual assurance that online transactions can be trusted. As an international organisation, OIX membership includes a cross-section of public and private sector bodies (eg Barclays, Google, Experian, Timpson). The Cabinet Office represents the UK Government.



OIX is a neutral, technology-agnostic, non-profit trade organisation where members can come together to share domain expertise and joint research, and to pilot projects to test use of real world cases to drive the expansion of existing online services and the adoption of new online solutions. Its goal is to enable the expansion of online identity services and adoption of new online identity products.

OIXUK is the UK arm, working directly with governments and the private sector to develop solutions and trust for online identity, specifically for the British citizen.

PRIVACY AND CONSUMER ADVISORY GROUP (PCAG)

This group is an independent voluntary body comprising privacy and security experts from across the UK. It provides the UK Government with independent expert review, analysis, guidance and feedback on all personal data and privacy initiatives by all departments, agencies and other public sector bodies. This includes GOV.UK Verify.

The group's remit is to ensure best practice in identity, privacy, security and technology to protect citizens' interests, with a particular focus on ensuring data and personal information, and the technology used to manage it, is well designed, engineered and implemented.

Outputs from PCAG, such as the nine principles of identity assurance (see Table 1), are valuable pieces of advice that enhance operational services. Councils might find it useful to reference such sources on their websites.

GOV.UK VERIFY

The UK Government has adopted GOV.UK Verify for central government service providers such as HM Revenue & Customs (HMRC) and, of particular interest for local public services, the Department for Work and Pensions (DWP). The Cabinet Office is also keen to explore the use of GOV.UK Verify in other areas such as further education, health, transport and local government, thereby reducing development costs and risks to these bodies and providing citizens with a single digital identity that can be used to access a wide range of government services online.

GOV.UK Verify is the responsibility of the Government Digital Service (GDS). It uses a range of identity providers (also known as 'certified companies', as they have to meet standards set by government) to check that users are who they say they are. Currently, four companies are connected: Digidentity, Experian, Post Office and Verizon. It is planned that they will be joined by five more (Barclays, Paypal, Morpho, Royal Mail and GB Group) before GOV.UK Verify goes live in April 2016.

The infrastructure of GOV.UK Verify is built to meet the privacy principles developed by PCAG and will ensure a greater degree of privacy than is likely through a locally developed solution. There are citizen service benefits that stem from a citizen having one properly assured digital identity that can be used to access both central and local government services: it is similar to having a corporate single sign-on to public services.

At the current time, GOV.UK Verify is in public beta for the following seven services:

- View or share your driving licence information (DVLA)
- Claim tax refund (HMRC)
- Claim for redundancy payment (Insolvency Service)
- Log in and file your self-assessment tax return (HMRC)

GOV.UK Verify is important because of the things that make it unique. It's been designed from the outset to be straightforward, secure and private. Government services can be sure that they're dealing with the right person each time, and users can be confident that their personal information is in good hands, and not stored in a single huge database.

That's because GOV.UK Verify works via certified companies, who check and confirm someone's identity before they use a government service. This happens completely online, and it's the first time this has ever been possible. Previous methods have always involved waiting for something by post, or going somewhere in person. And it's fast: it takes about 15 minutes the first time you verify your identity, and less than a minute each time after that.

Source: [Why GOV.UK Verify matters](#)

- Claim rural payments (Defra)
- Help friends or family with their tax (HMRC)
- Check or update your company car tax (HMRC)

[A further 30 government services are planned to be implemented by April 2016.](#)

Discussions are taking place with NHS England about extending GOV.UK Verify for patient access to medical records. As this briefing was being prepared, it was reported that initial feedback from some patients invited to test this new service indicates a degree of unease when they heard about the use of third parties such as banks as identity providers. This suggests the need for great care in dealing with social care clients and carers.

4. LOCAL GOVERNMENT PRACTICE

LOCAL SOLUTIONS

In contrast with central government, there is as yet no national solution available. Although GOV.UK Verify is not yet available for local authorities, the service has been built to make that possible. Some councils have developed local solutions in response to needs of individual services such as revenues and benefits where payments are made. These are rarely more than user name and password systems, not extending beyond level of assurance one (LOA1). A few council systems also include one security question (eg mother's maiden name), provided by the user on registration.

Moreover, there is no corporate approach to many of these initiatives. As a result users may have to repeat the process for different services within the same council, even for such transactions such as reporting a change of address, where it is reasonable to expect to have to do this just once.

THE WARWICKSHIRE EXEMPLAR

One council has, however, aimed higher. Warwickshire County Council (WCC) has worked over the past two years with GDS, DWP and authentication partners in the commercial sector to prototype a scheme for applying for (or renewing) the blue badge for a disabled person's car parking permit.

We make no apology for devoting over three pages to illustrate this exemplar for a number of reasons:

- This replaces in a single online transaction a labour-intensive, back-office paper trail leading to delays in citizens receiving their blue badge.
- It is the only example in England of a council working with central government to produce a service that has built in authentication to LOA2 and that might also be used by other councils.
- It is an application relevant to adult social care.
- The service is clear, well-designed and well-tested.
- Appropriately for a sensitive application, user reactions have been analysed in detail and helped to shape the service.
- Only by seeing a step-by-step analysis of the process can one understand the attractiveness of the solution from the user viewpoint.
- In every respect it sets a benchmark for all approaches to identity and authentication.

A report, *Towards an architecture for a digital blue badge services*, published in late August 2015 by OIX, documented the results of the prototype.

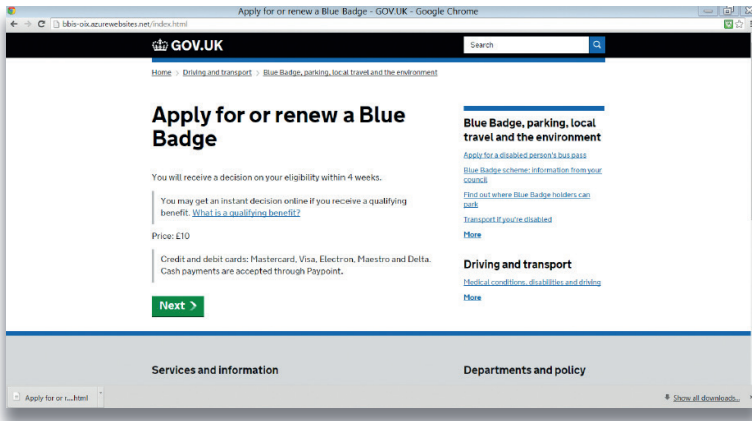
Here we reproduce from the main report the key steps in the new process for applying for a blue badge.

01. Welcome and context setting
02. Verification of identity
03. Capture of eligibility criteria
04. Confirmation of eligibility with DWP
05. Obtaining of digital ID photograph
06. Declaration
07. Payment and finish

STAGE	START	END	PARTNERS WITH GDS AND WCC
WCC 1 Alpha	Mar '13	Oct '13	Innovate Identity, PayPal, Mydex and Verizon
WCC 2 Discovery	Dec '13	Sep '14	Innovate identity, Mydex and Verizon
WCC 2 Alpha	Feb '15	Aug '15	DWP, Innovate identity, Mydex, Northgate Public Services and Verizon

Table 2 History of project

STEP 01



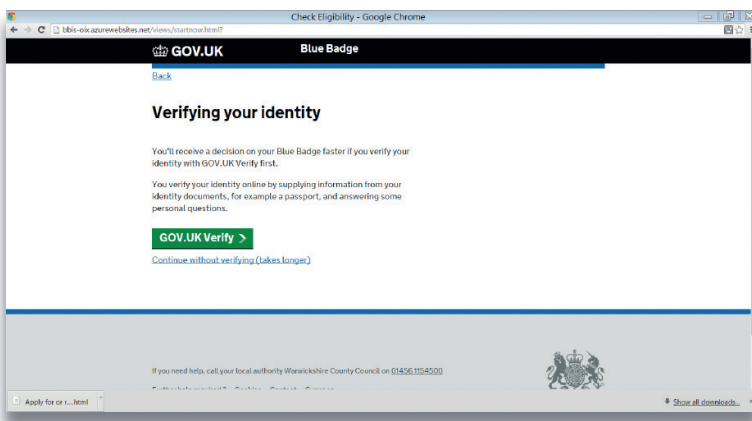
WELCOME AND CONTEXT SETTING

This screen is where the user journey starts. The user is made aware that a payment will be required. The next screen (not shown) informs the user that an ID photo will also be required.

USER REACTIONS

The natural inclination of most users was first to click on the link on the right of the screen to find out more about the Blue Badge scheme before proceeding with the application. They automatically went for “trigger” words such as “Council” and “Blue Badge”. The large “Next” button at the bottom of the page was not a clear enough call to action.

STEP 02



VERIFICATION OF IDENTITY

Before the Blue Badge application process can commence, the user is required to identify themselves through Verify. This screen leads to the Verify Registration or Sign-in screen (not shown).

USER REACTIONS

While respondents understood the need for the eligibility of applicants to be checked, so that Blue Badges were not obtained fraudulently, the role of GOV.UK Verify in this process was often unclear (among those respondents who went through registration). Most users who were taken through the registration process were accepting of the practice of using documents such as the passport and driving licence as a means of identity verification. Knowledge-based authentication, however, using financial information as a means of anti-impersonation checks, was confusing and many respondents had problems in associating this with the identity-checking process. One user thought this was a way to obtain a credit record, which they welcomed! Another user thought they were being means-tested in relation to the £10 fee for a Blue Badge.

STEP 03

Section 2 of 5
Your eligibility

Please tell us if any of the following apply to you:

Are registered as blind (severely sight impaired)	Yes	No
Have either a valid Certificate of Vision Impairment (CVI) or a valid BDR form - based on an optician's report	Yes	No
Receive the Higher Rate of the Mobility Component of the Disability Living Allowance	Yes	No
Receive a Personal Independence Payment (PIP) and meet a PIP Living Allowance descriptor for the Mobility Component	Yes	No
Receive a UK Pensioner's Mobility Supplement	Yes	No
Receive a tariff within 1-6 (inclusive) of the Armed Forces Compensation Scheme and have been assessed as having a permanent and substantial disability which causes inability to walk or very considerable difficulty in walking	Yes	No

[Next](#)

CAPTURE OF ELIGIBILITY CRITERIA

Users who can answer “Yes” to one or more of these eligibility questions automatically qualify for a Blue Badge. On clicking <Next> the user is presented with a panel that asks for their permission for this eligibility to be checked with DWP (not shown). On giving permission, the attribute exchange process is enacted through the attribute exchange hub.

USER REACTIONS

Most respondents were entirely comfortable with providing this information and giving their permission for their eligibility details to be checked. They recognised that this was to prevent fraudulent applications and welcomed this. Some users happily recounted situations where they had witnessed a Blue Badge being used fraudulently, and approved of measures being taken to prevent this. Other respondents, however, were unhappy with the act of giving permission. For one this was because of anxiety about Verify – she perceived that the attribute exchange permission would signal her assent to the Verify process, with which she was uncomfortable. For others, the permission request seemed unnecessary and onerous – one more click in a long journey (made long by Verify registration, among other things). These findings show the potential vulnerability of attribute exchange: user acceptance of it can be affected by the context in which it is encountered.

STEP 04

Section 2 of 5
Your eligibility

You are eligible for a Blue Badge

DWP has confirmed that you receive a disability benefit that makes you eligible for a Blue Badge

[Next](#)

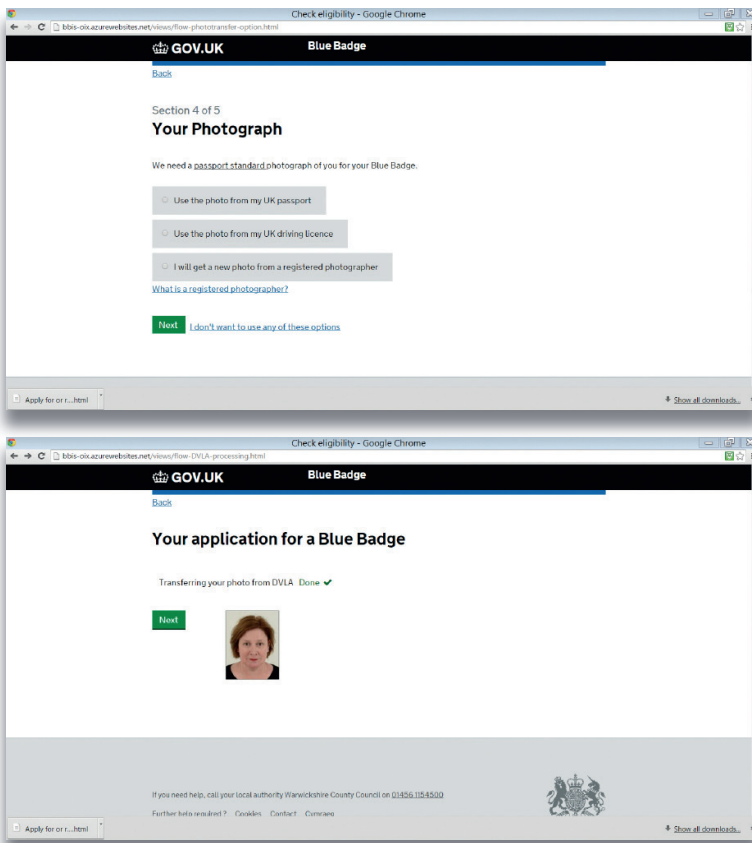
CONFIRMATION OF ELIGIBILITY WITH DWP

The attribute exchange process takes place and confirmation is obtained from the DWP that the eligibility criteria are correct.

USER REACTIONS

Users understood the checks taking place and generally thought “that was good”.

STEP 05



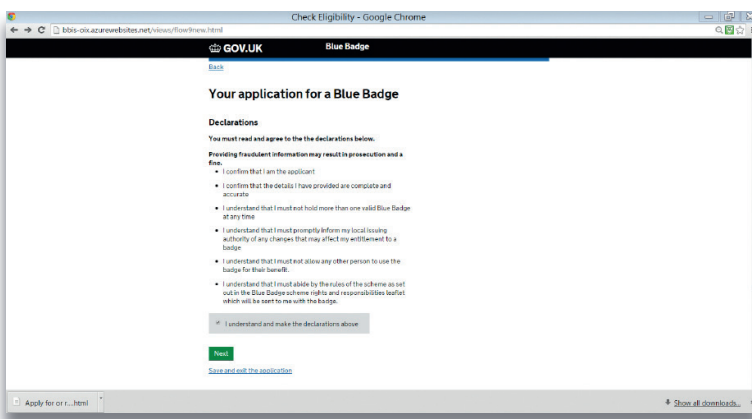
OBTAINING OF DIGITAL ID PHOTOGRAPH

The user needs to provide a digital ID photo. In the user journey three options were provided, with users being given the choice of which option to choose. In the prototype the driving licence option is enabled and permission is sought (not shown) to obtain their photo from the DVLA.

USER REACTIONS

Respondents who obtained their photo from their passport or driving licence were generally clear about and happy with the photographic evidence part of the journey. Those who opted to obtain a new photograph from a registered photographer were much less happy, because the latter route was much harder to understand and seemed more onerous (particularly for respondents who had health or mobility problems). Respondents who opted for the driving licence/passport route were generally happy to give permission for the photo to be obtained in real time from these sources (although, again, some felt that this permissions request was unnecessary). Being able to see the transferred photo drew positive reactions and comments.

STEP 06



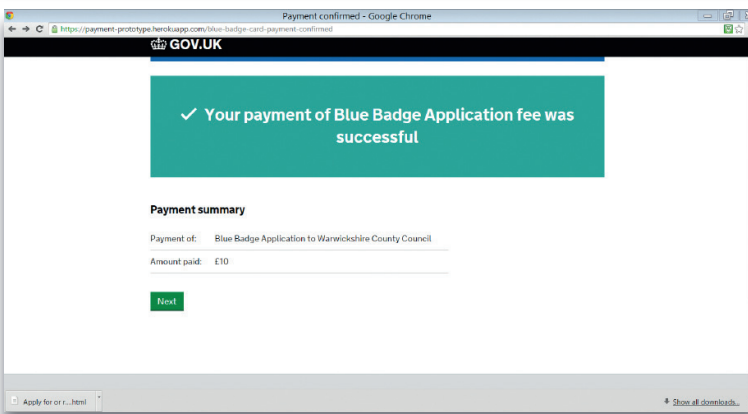
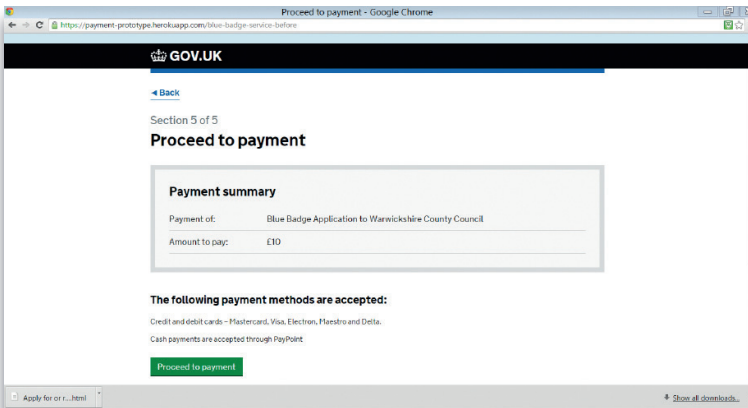
DECLARATION

The user is required to declare that they understand what constitutes a fraudulent application and the consequences of making such an application.

USER REACTIONS

Most respondents expressed no objection to the presence of the declarations (with the exception of one, for whom they were over-long and unnecessary); and for some they were a welcome additional anti-fraud procedure. The declarations were read with varying degrees of attention by respondents – some gave them a close reading while others gave them just a very cursory inspection.

STEP 07



PAYMENT AND FINISH

To complete the application a payment of £10 is required. Several payment options are available. The user is required to enter their chosen payment option and details as part of a typical online payment process (not shown).

USER REACTIONS

All users were familiar with online payments, although some may ask family members to make payments on their behalf. All selected the debit/credit card option. No users were familiar with the PayPoint option, perhaps reflecting the demographic used for the research.

BENEFITS OF EXEMPLAR

The service is a major improvement. The benefits, too, are clear. It will reduce waiting time for a blue badge from weeks to minutes. In Warwickshire, reversing the current online to offline take-up ratio of 13% : 87% to 87% : 13% would both reduce citizens' costs (eg postage, photocopying) by 75% or nearly £5 per application, and save the council £130,000. Repeated nationally, the savings would be nearly £12m.

The emphasis on user reactions helps to build confidence in the usability of the system. Identity and authentication is clearly a sensitive topic for any user of public services. Involving users at key stages of the design of the user journey will increase acceptance and ownership. It is critical to keep the user journey as simple as possible with exactly the right words in the right place.

5. OPTIONS FOR LOCAL SOLUTIONS

EXTENSION OF GOV.UK APPROACH?

It is interesting that streamlining the identity and authentication forces a redesign of the whole process and points the way clearly to a national solution for all local authorities. As it happens, applying for blue badges already follows national rules, but many other local services that require better authentication may follow local rules (eg applying for disabled parking bays). In such cases it is likely that national solutions might emerge in order to incorporate better identity and authentication. There are major customer benefits to a single identity assurance approach across the whole public sector rather than a piecemeal approach.

When will it be available? This is the critical question where the catch is.

In the language of Agile, the blue badge prototype is an alpha project needing further work to turn it into an operational system. The project report from GDS and OIX lists six recommendations that range from improving the documented weaknesses (eg the need for some applicants to take a new digital photo rather than use an existing one from passports or driving licences) to converting the prototype attribute hub into a full production platform. It will take months to implement the recommendations.

Even then it will only be a partial solution for blue badge applications that covers the 40% of applicants who can be fast-tracked by virtue of already being registered partially blind or qualifying for another benefit. It excludes the 60% who would have to provide new documentation to prove their eligibility. This, too, will take months to implement.

For any of this work to come to fruition, it is essential that local government gains access to GOV UK Verify. This provides the essential anchor of trust to underpin attribute exchange. GDS is understandably devoting all its Verify resources to convert all the current beta services to fully live services in 2016.

For the Warwickshire exemplar to be implemented and extended to other applications, it is vital that those applications are given the time and resources. Currently, there is no funding for such an extension to local public services and the full details of the impact of the recent Comprehensive Spending Review in this area are not known at the date of publication.

It is estimated that there might be as many as 50 applications that such an authentication process would cover for all local public services. If we want adult social care services to be high on the priority list, then we must build a strong business case for how those services could be transformed. Such an exercise might also usefully consider potential benefits from a single identity and authentication process from integrating health and social care.

Taking all these points into consideration, we might estimate that it will be two or three years at least before we see any national identity and authentication solutions for any adult social care application.

AN NHS EXTENSION?

It is possible that a similar approach might develop from current NHS initiatives.

Since April 2015, you can look at your GP records on a computer, a tablet or a smartphone, using a website or an app. You can choose to book and cancel appointments online with your doctor or nurse, and you can order repeat prescriptions.

At the moment, you need to register in person at your GP surgery to use these online services. Your surgery will need to check who you are to make sure you only see your record and not someone else's. They will do this by face-to-face/manual authentication, after which your surgery will give you a letter with your unique username and password. It will also tell you about the website where you can log in and start using online services.

The NHS goal for March 2018 is for all individuals to be enabled to view their care records and to make their own comments and preferences on their record, with access through multiple digital services. Initially, this will focus on data held by NHS providers (primary care, acute, community and mental health), and it will be progressively extended to cover other care settings, taking account of the work that local authorities are progressing in regard to personal records. This will create the opportunity for individuals to create and manage their own personal care record.

The NHS Citizen Identity programme sets out to enable people to verify their identity once in order to obtain a digital identity that can be used to access records and services across health care providers such as GPs, hospitals and social care. A typical case is a person with a long-term condition who would self-care more effectively with access to their data, such as test results, care plans and medicines.

Its approach builds on the GOV.UK Verify solution by looking to establish a federated identity scheme with multiple methods of verification, ie in person or by Verify for example, as it recognises that not everyone will want to or be able to use Verify.

CAMDEN: NHS AND COUNCIL COLLABORATION

Camden Council is currently exploring options with Camden Clinical Commissioning Group (CCG) for devising a practical solution within its area that enables both citizens and patients to use the same authentication processes across council and health services. Camden already has a corporate online customer account covering five major services which enables residents to establish their identity via a user name, password and one prompt to establish credentials (eg mother's maiden name).

As part of this investigation, the council supported by NHS England is looking for a solution that might be the basis of a national blueprint for use by NHS agencies, councils and other service providers. Such a solution might become an alternative solution to GOV.UK Verify for local public services.

HAMPSHIRE

The University Hospital, Southampton is planning a pilot in early 2016 for enabling federated access to services by patients to access records across the Hampshire Health Record. This is an integrated record for use by professionals which aims to include social care data as well as medical data.

LIVERPOOL

Liverpool is building a patient-facing service that can interoperate with verified identities sourced from either Verify or a local verification process. This project entails Liverpool CCG joining the GDS contract to use the certified identity providers. A pilot also starts in January 2016.

Given that any different approach that might emerge from an NHS source is only at the early stages of investigation, such an option might also be at least two or three years away from any national implementation.

ONLINE CUSTOMER ACCOUNTS?

Some councils, especially those with adult and children's social care functions, may not want to wait for a national solution for local public services, however sourced. How can they move forward with improved identity and authentication?

One obvious source of solution lies with the development of online customer accounts. Such an account enables citizens to be known online to the council, usually by their email address, and to return online with that identity to track or update their individual information.

We know from Socitm's *Better connected* research that some 40% of the 152 councils in England with social care functions already have an online customer account and that the number is gradually increasing from year to year. However, this may not be a truly corporate account but restricted to a few, or just one, major service. Moreover, we also know that very few, if any as yet, include social care applications, as they are focusing on applications that are either high volume or relatively simple, such as benefits, council tax, email alerts, planning, fault reporting or rubbish collection.

Suppliers of software for supporting online customer accounts are gradually making their facilities more sophisticated and developing authentication processes that enhance their core product (eg by adding to customer relationship management systems or e-forms systems). At least one supplier has a facility whereby a person already possessing an online account for one simple application has to establish their credentials when applying for a new application for the same account. This is done by using a list of customisable options (eg four digits of a bank account code).

For councils that have such a corporate online account the degree of sophistication of authentication processes will be determined by the software that they already have in place. Those without such a facility should now be able to influence the selection of the software using criteria that include ease of use and quality of authentication, which almost certainly did not happen before.

For those who do not want to wait for a national approach to emerge, there may be scope for developing current applications with stronger identity and authentication functions from a current base of an online customer account.

If that is not feasible, then you may be able to implement an adult social care line of service solution. Some suppliers offer citizen transaction facilities that can be effectively incorporated into the council website with consistent branding and include a dedicated social care account with authentication.

DO NOTHING?

If a national scheme is not available in a practical sense, and no obvious local solution materialises for another purpose, then adult social care services have nowhere to turn for help with identity and authentication. However, this need not be as negative as it sounds.

There is a sense in which online services have developed without the need for comprehensive authentication: most people used to online working in their private lives are quite comfortable with buying products and services with little more than user name/ password authentication. In these ‘payment involved’ scenarios, the key authentication step is via the online payment system, which is the concern of a third party, eg a credit/debit card issuer, and not of the public service consumer or the provider per se. The financial services provider is sure to look well after its own interests.

Different public services require different levels of authentication. Councils can make progress in developing many online facilities without having comprehensive authentication where this is just not required. Even those services that would benefit from greater authentication (eg apply for blue badge) can arguably function perfectly well without, as they do now.

POTENTIAL APPLICATIONS FOR DISABLED PEOPLE

DISABLED PERSONS	
TASK	
①	Apply for free (or reduced rate) rail card
②	Apply for free transport etc for authorised helper
③	Apply for bus pass
④	Apply for financial assistance
⑤	Apply for parking bays
⑥	Apply for parking permits
⑦	Apply for taxi cards
⑧	Apply for identity cards
OTHER CATEGORIES OF USERS	
USER	TASK
⑨	Businesses Register adult day-care service
⑩	Carers Claim for carer’s allowance
⑪	Older people Apply for bus pass

Table 3 List of possible applications
Source: Warwickshire CC using LGA data

We reproduce here an extract from the LGA list of local government services, annotated by Warwickshire CC to highlight those services that might benefit from identity and authentication.

PLANNING FOR IMPROVED AUTHENTICATION

Whatever options are considered, then this is the time to make plans. Each council can produce a plan based on the services that would benefit from greater or lesser authentication on a case-by-case basis. Each will need to make its own assessment of the transactions that they are moving online, the degree of risk they pose and the level of risk mitigation necessary. Many transactions can be carried out without any form of identity assurance at all. Others may be deemed to rely on simple 'known facts' (council tax reference, National Insurance number, etc). It is the remaining transactions requiring higher levels of identity assurance that are key to the business case for LOA2 and higher identities.

In general terms, these services relate to financial claims or benefits eligibility. If councils are paying out benefits, claims or refunds, they have to be sure that the payee is the right person. The same applies to establishing eligibility for benefits that are indirectly financial (eg blue badges and any council-funded social care service). However, the offline delivery of the service to a particular address and person may be considered sufficient confirmation of real-life identity.

There may also be a new issue to face that is not covered by simple services, or even the more complicated blue badge application. This covers situations where third parties such as carers for a number of possible reasons are acting on behalf of applicants who are not capable of acting for themselves. In the longer-term authentication would have to cover such cases. Even with their many services now in public beta GDS has not yet progressed beyond the stage of exploring the issues, preferring to focus on the common case of people acting on their own behalf.

This issue may also include groups of 'allied professionals' (eg community nurses, GPs etc.) who form part of the circle of care around an individual; they may also require some similar or complementary mechanism for assuring identity. More broadly for networks of less regular, informal carers, additional levels of authentication which allow for verification of identity, relationship to the subject and other key areas of assurance such as mental capacity and safeguarding will also require future consideration.

Specifically, each council should review the authentication of their existing online services for adult social care to see if these are fit for purpose. They should also assess their plans (over the next five years) for putting further services online to see if they are robust for appropriate levels of authentication. For each service they should consider:

- the level of assurance (LOA) required, including 'None'
- the type of transaction (eg pay for service, receive payment, request service, find information)
- the likely implementation date
- the likely level of identity assurance required
- the likely solution (eg national, or locality-based online customer account)
- the probable savings and improvements that might be achieved.

From this one can draw out a priority list for development. Those payment or eligibility applications requiring the greatest authentication may be able to wait for national solutions similar to the blue badge exemplar in this briefing. Or you may be able to implement a corporate solution or one from your social care software supplier.

6. CONCLUSIONS

Identity and authentication matters are a critical aspect of secure and trusted online interactions and transactions. In the UK, as elsewhere, they have been the subject of long and sometimes difficult discussions for many years. The devil is in the detail of practical application, not in the theory of how to build such systems.

In the past three years we have seen the gradual development of a credible local authority exemplar by Warwickshire CC, which we have analysed in some detail in this briefing. This has the potential for handling the more complex cases from LOA2 and above. Now a working prototype, it might, however, be at least another two years before it can be turned into a scalable, viable national solution that can then be replicated across other applications.

It is possible that a similar solution might emerge from current ideas at Camden and elsewhere that would cover health services, but these are much less well developed.

Some councils have implemented local solutions over the past three to four years, based on online customer accounts in response to more pressing needs in other services. As yet, they have barely touched adult social care.

In the meantime, councils may need to adopt a pragmatic local approach, prioritising transactions where lower levels of authentication are required and, where they exist, working with corporate online customer accounts. They may also find that suppliers of adult social care online systems include their own adequate identity and authentication processes, eg use of a code issued via a mobile phone as a second factor.

Although progress has been slow, now is the time to produce a detailed plan for the implementation of identity and authentication schemes which recognise the different degrees of risk from insecure processes. At least this will ensure that the organisation is ready when solutions, national or local, mature.

NEXT STEPS FOR YOU

- Keep a watching brief on any national solution that develops from the Warwickshire prototype on blue badge applications and from other initiatives involving NHS England.
- If your council has already invested in a corporate system that provides an online customer account, investigate any current or planned authentication functions that you might be able to use.
- If your council has not yet invested in such a system but intends to, make sure that both authentication functions and ease of use are built into the requirements.
- Consider producing a five-year plan for identity and authentication relevant for online social care facilities.
- Ensure that any local identity and authentication solutions use a federated model based on industry standards.
- Start to build the business case to show how identity and authentication as part of a move to more online self-service might transform the delivery of social care services.

FINAL ACTION

If your council is making strides with identity and authentication, then do let us know so that we can keep your colleagues updated.

Email: richard.pantlin@adass.org.uk

FURTHER INFORMATION

Government (GOV.UK)

Why GOV.UK Verify matters

<https://gds.blog.gov.uk/2015/09/23/why-gov-uk-verify-matters/>

Good practice guides (GPG) jointly from CESG, the UK's National Technical Authority on Information Assurance, and GDS (Cabinet Office):

- *Requirements for secure delivery of online public services* (GPG 43)
- *Authentication and credentials for use with HMG online services* (GPG 44)
- *Identity proofing and verification of an individual* (GPG 45)

Open Identity Exchange

<http://oixuk/org.uk>

- *Towards an architecture for a digital blue badge service* (August 2015)
- *A technical design for a digital blue badge service* (August 2015)
- *Can attribute provision, together with identity assurance, transform local government services?* (September 2014)
- *Economics of identity* (June 2014)
- *Interoperability between central and local government identity assurance schemes* (October 2013)

Socitm Insight

www.socitm.net

- *Identity assurance: enough on its own?* (Briefing 69, September 2014)
- *Open Identity Exchange: a basis for trust?* (Briefing 61, January 2014)
- *Knock, knock: who's there?: an overview of authentication for electronic service delivery* (November 2004)

Engaging Citizens Online

List of briefings: topics

-  **01** *Identity and authentication*
-  **02** *Methodology for developing the online user journey*
-  **03** *Business case for digital investment*
-  **04** *Planning online transactional facilities*
-  **05** *Supplier offerings of social care self-assessments*
-  **06** *Supplier offerings of social care financial assessments*
-  **07** *Examples of effective use of national information sources*
-  **08** *Examples of good practice of e-marketplaces in operation*
-  **09** *Promotion of online services*
-  **10** *Role of third sector and care providers*