

## Employee Authentication for Local Authorities via Government Connect

Revision 3.

Compiled by Paul Davidson, LeGSB

30<sup>th</sup> July 2007.

### **Change Control**

<b>Revision</b>	<b>Date</b>	<b>Notes</b>
1	26/7/07	Presented to the DLCG/DCSF Community of Practice workshop for Level 2 Employee Authentication. Drawn from comments received from ....  John Smith, Leeds City Council, representing the West Yorkshire Partnership Rosemary Turner, St.Helens Council Paul Davidson, LeGSB and CIO Sedgemoor District Council.
2	30/7/07	Reformatting to place the information into a logical order.
3	30/7/07	New contributions from  Angharad Jackson, Salford City Council Bob Busby, Derbyshire County Council  Salford, and Derby.

### **Purpose of this document**

The DCLG/DCSF Community of Practice Working Group for Local Authority Employee Authentication, at their meeting on the 20<sup>th</sup> July 2007, asked for the Local Authority representatives to come forward with context and information to inform the group to develop 'requirements' for a solution. This document captures and collates the contributions that have been made.

This document should underpin the development of requirements for 'authentication' to enable individuals to represent Local Authorities when accessing ...

- Information from Contact Point in particular
- Information and services from other Government sources

... and look for further opportunities for convergence such as ...

- Single Sign-on within a Local Authority
- Supporting the notion of Shared Services
- Enabling information and services governed by Local Authorities, to be accessed by the wider public sector.

### **What is ContactPoint?**

It will be the quick way for a practitioner to find out who else is working with the same child or young person, making it easier to deliver more coordinated support.

It will be a basic online directory, available to authorised staff who need it to do their jobs. It is a key part of the Every Child Matters programme to improve outcomes for children.

Source: <http://www.everychildmatters.gov.uk/deliveringservices/contactpoint/>

### **How will users access ContactPoint Information?**

The number of users is estimated to be around 330,000 and will include practitioners from education, early years and childcare services, Connexions, health, social care, youth offending services and police. Others, including the voluntary sector may also be granted access depending on their role.

Authorised users will be able to access ContactPoint in three ways - through:

- A **secure** web link
- Some existing case management systems
- Another authorised user (where appropriate IT is unavailable)

Source: <http://www.everychildmatters.gov.uk/deliveringservices/contactpoint/>

### **From the ContactPoint Security Policy**

Access will be **strictly restricted** to those who need it as part of their work

... not every practitioner working with children and young people will be given access

Before being granted access to ContactPoint, users will be required to have a current (not more than three years old), enhanced **Criminal Records Bureau** certificate, membership of and subject to monitoring by the forthcoming **Vetting and Barring Scheme**, and be **trained** in the safe and secure use of the system, including compliance with the Data Protection Act and Human Rights Act.

Practitioners will be made aware that their use of ContactPoint will be continually audited and patterns of activity that may indicate misuse will be further investigated.

There will be cases where a practitioner does not have direct access to the information held on ContactPoint. This may be because they do not have access to a PC or laptop, or they may be working away from their office. It will therefore be necessary for them to contact someone who does have access, and who can perform queries on their behalf (mediated access). The person with direct access will only release information **once they are satisfied that the person seeking information is authorised** to receive it and has given a genuine reason for accessing that information. Auditing this kind of mediated access will include recording the identities of both parties.

Firstly, strong **2-factor authentication** will be used involving **something a user has** (token) and **something the user knows** ...

Source: ContactPoint Security Policy,  
[http://www.everychildmatters.gov.uk/\\_files/9202DFBC293F35D7E57EB2F01932D936.pdf](http://www.everychildmatters.gov.uk/_files/9202DFBC293F35D7E57EB2F01932D936.pdf)

## High Level Conclusions and Recommendations.

As a part of this exercise, some Local Authorities were asked a standard set of questions. The answers are reproduced in Appendix A. Some of the conclusions are reproduced here, within each step of an authentication process.

### **Adoption, Take-up, Impact, Environment**

#### **Conclusions**

The Business Case for adoption by District Councils may be unattractive, as it will only affect a handful of staff. For all other types of Council, this is core business.

For a typical council ( other than a District ), this might require that 10% of the staff are authenticated in this way.

Authorised access is required by

- Direct Employees of a Local Authority
- Employees working under contract to a Local Authority
- Secondees, employed by other agencies, but working within a Local Authority.
- Employees of an organisation which has been empowered by a Local Authority to represent it ( e.g. Outsourced processes )
- Employees of an organisation which looks to a Local Authority to facilitate access, but which does not represent the Local Authority ( e.g. Some Voluntary Sector organisations ).
- Employees of organisations delivering services locally, other than a Local Authority. ( e.g. Health, Police ).

Some, non-public-sector organisations may not be connected into a secure Government Extranet. ( e.g. GCSx. ).

It is unclear how a 'mediator' will determine if a person has the right to access ContactPoint information.

Local Authorities will want to have a single approach to

- Verifying the Identity of those that represent them
- Issuing a credential associated to a verified identity
- Managing the life-cycle of an issued credential
- Associating further attributes to a verified identity
- Enrolling a verified identity to be able to carry out a specified process
- Challenging for authentication
- Authorising access to information or a service
- A code of connectivity for accessing resources over a Government extranet.

There are a number of current initiatives that are sponsored by Central Government, that will require that Local Authority staff are authorised to access information or services. Some of these are listed at **Appendix B**. There is a risk that these solutions will not converge to be a single set of processes, standards and technologies.

Individual Local Authorities are being invited by the DCSF to champion the development of each existing Case Management product, to support the needs of ContactPoint.

Some Local Authorities have already been given an expectation regarding the nature and source of 'level-2' tokens, for ContactPoint.

Successful deployment of ContactPoint will depend on many deliverables other than those within this Working Group.

Local Authorities will be concerned about the dependency and resilience on externally provided facilities that might impact on a Local Authority's ability to carry out its duties.

Local Authorities will want to know the set up costs, and the ongoing costs of operating employee authentication. Where applicable, these costs should be attributable to each service area.

Local Authorities will want to be provided with a realistic timetable for delivery, and with clarity over what will be delivered.

## **Recommendations.**

Verify the list of target employees above.

Consider if '*Employees of organisations delivering services locally, other than a Local Authority. ( e.g. Health, Police )*' are in scope of this initiative.

Seek clarification from ContactPoint as to what is acceptable during mediated access to authenticate the identity of a user who may make a request by phone, or in person.

Local Authorities selected by DCSF to represent existing Case Management systems, should be facilitated to exchange requirements with this Working Group, about

- Standards, Formats
- Interfaces
- Access to Test Facilities

The group ( presumably in DCSF ) that owns the successful roll-out of ContactPoint should be identified and a relationship put in place so that dependencies and risks can be shared.

A fall-back position for providing access to ContactPoint information, should be developed in parallel, in case the general authentication solution cannot be delivered in time.

The channels by which progress on Employee Authentication, and ContactPoint are communicated to Local Authorities and suppliers, should be identified and quickly used to lay out the method of approach, timetable for delivery, pre-requisites and costs.

The 'landscape' of Government initiatives that will require authenticated access from Local Authorities should be mapped so that ...

- A consistent and confident message is given to Local Authorities

- Convergence of processes and technologies is a design goal.

The 'mapping' of other initiatives should establish if information is to 'flow' the other way, such that Central Government departments are able to access Information and Services from individual Local Authorities.

A 'Risk Assessment' should be performed to consider the necessary 'availability' and 'performance' characteristics of the required service. An SLA should be constructed that meets the requirements of the assessment which should form a part of the specification of requirements of the solution.

Local Authorities should be canvassed for their opinion on the acceptable cost of operating the solution, and that should be factored back onto the evaluation criteria.

## **Verification of Identity**

### **Definition**

The steps necessary to establish the identity of an individual to the level of certainty required.

### **Conclusions**

Local Authorities will verify the identity of its own directly employed staff. For staff from other organisations who are empowered to represent a Local Authority, either

- The Local Authority will perform the Identity Verification process.
- The empowered organisation will perform the Identity Verification

The 'information or Service owner' will prescribe the pre-requisites for access. Therefore, a minimum acceptable Identity Verification process will be required to be adopted across the Public Sector.

A single 'Identity Verification and Registration' process will be required across all organisations that register staff.

Local Authorities are subject to a number of controls when verifying the identity of staff, including

The Asylum and Immigration Act 1996 makes it a criminal offence to employ someone who does not have the right to work within the UK

Section 12 of the Children Act, where further checks must be repeated every 3 years.

### **Recommendations**

Develop a policy to be consistently adopted to define the process that Local Authorities must go through to verify the identity of their direct staff,

and those that are empowered to represent them. Look to have this policy adopted across the UK Public Sector.

Identify the right association through which Local Authorities might be engaged on the development of an Identity Verification Policy, and facilitate via that group. ( e.g. ALARM – The association of Local Authority Risk Managers. )

Development of a Registration Policy is NOT dependant upon the authentication solution, and therefore, it should be started immediately.

Clarify if there is an expectation that Local Authorities will be required to verify the identity of staff other than those it directly employs, e.g. Outsourced processing.

## **Registration**

### **Definition**

How a 'credential' is associated with an identity

More than one 'credential' may be associated with a single identity, to provide more than one level of Authentication, so that a single user can authenticate at different levels dependant upon the authentication capabilities of each service provider.

The further management of the credential

- Revocation

### **Conclusions**

Local Authorities are at various stages of roll out of local implementations of 'Single Sign-on'. Some have already issued Level 2 credentials to their staff; some have no level 2 credentials and have no single-signon approach to accessing applications.

Many line-of-business computer systems issue their own credentials. 'Single Sign-on' to application systems via local directory services has not been universally achieved.

Existing 'HR' systems may not record sufficient information to rely on as assurance of a verification process. HR information may not be recorded to the level required as Records Management.

### **Recommendations**

The solution should contain facilities to enable participating organisations to register staff, i.e. act as a Registration Authority.

Consideration should be given as to how Local Authorities may record verification data along with the credential to which they are associated.

Registration Authorities should have the choice of which credential to issue, so long as it is associated with a 'level-2' identity verification process ( as defined by this project ), and so long as it meets the requirements of 'level-2' when it is presented for authentication ( 2 factor ). However, the solution should also provide facilities for Registration Authorities to issue credentials, where no existing capability exists, or, where it is advantageous to use a centrally devised solution.

A mixture of 2-factor credentials should be permissible by using globally accepted Identity Management and Federation standards.

The credential should be re-useable across a number of scenarios.

Consideration should be given to the pros and cons of making the credential portable, such that it may be used to authenticate to a network other than that which issued it.

## Enrolment

### Definition

How a 'registration' is associated with a 'service', and potentially, the rights to certain individual 'accounts' or 'documents'.

### Conclusions

Local Authority employees will be explicitly identified as requiring access to a process, by a Council's Line Management. The notion of 'Roles' does not seem to add value.

An employee of a non local authority organisation may be empowered to represent more than one Local Authority.

Where an organisation is empowered to represent a Local Authority, it is not clear if the Local Authority will give explicit rights to each individual, or if the empowered organisation will do that.

### Recommendations

The service provider should be able to make each **process** visible so that employees can be explicitly 'enrolled' to gain access to it.

Consideration should be given as to how each Service provider will define the attributes upon which it will consider if access is to be authorised. E.g. qualifications and clearances.

Consideration should be given as to how each Service provider will trust each organisation to enrol the appropriate staff, with the right clearances and qualifications.

A controlled list of attributes should be developed, so that qualifications and clearances can be asserted using a shared vocabulary. Without this, a service provider will not be able to define their requirements, and will not be able to check that an individual has met those requirements in an assertion.

Facilities will be required to enable a Local Authority ( or an empowered organisation ) to enrol their staff by explicitly giving the right to represent the

Authority when using a Service Provider's process. Note that it is possible that the Service Provider may refuse to provide that access during the Authorisation phase.

These facilities should include the ability to record further attributes for each individual, such as clearances and qualifications, and further manage their renewal and expiry.

The facilities should also check that the individual has met the minimum requirements for clearances and qualifications as defined for each process by the Service Provider, before allowing the Enrolment to complete.

Where access is required by an individual to represent an organisation other than the one that performed the registration, consideration should be given as to which organisation will be able to do this enrolment. I.e. The Local Authority being represented, and/or the organisation employing the individual.

Consideration should be given as to how the 'enrolment' commits an employee to the Terms and Conditions of use of the Service

## **Authentication**

### **Definition**

The verification of a credential as it is presented, in order to gain access to the services to which the associated registration has been enrolled.

The 'level' of the resulting Authentication will be the lower of

- The 'level' of the identity verification applied to the registration
- The 'level' of the nature of the credential

### **Conclusions**

### **Recommendations**

The Trust model should be determined and expressed in terms of what is being asserted by a successful authentication. E.g.

e.g. This access is made by

- an identifiable individual
- who is empowered by an identifiable organisation
- to represent an agency ( which may not be their own )
- to access an identifiable process
- who has met the requirements stipulated by the service provider
- and who has undertaken to protect the information as required by an existing agreement

The points in a public sector architecture at which the authentication may be made, should be determined, and where they occur within the domain of an employer, the globally accepted standards that enable the authentication to be federated should be stipulated.

Consideration should be given to, who will authenticate, and to which services e.g.

which of the following are included ...

- a Local Authority employee accessing information at another Local Authority
- a Local Authority employee accessing information at a central Government Agency.
- An employee at a non Local Authority agency ( say a health worker ) accessing information at a Local Authority

## **Authorisation**

### **Definition**

The ability to check that an Authenticated Session has the rights to access a requested process, account, document etc.

### **Conclusions**

There will be circumstances in which access to information may be restricted to individual cases, rather than just the nature of the information.

### **Recommendations**

Where appropriate, a mechanism will be required for an Agency to propose that an individual employee should be given access to an individual case.

The Service Provider will need to maintain a record of the individuals who have been explicitly granted access to individual cases.

Contact Point should develop a set of 'Terms and Conditions of Use' to cover the use, storage and onward distribution of information provided by ContactPoint. The enrolment process should provide evidence that an employee has signed-up to these.

## **Facilities that could be provided to Local Authorities**

### **Deployment**

In assessing existing assets, and procuring additional components of a solution, the following functionality might be either ...

- Provided via Government Connect via a quick-start computer application for deployment within a trusted domain ( i.e. deployed by a Local Authority ),
- Provided via Government Connect and deployed centrally, accessible over GCSx
- Described in terms of standards so that Local Authorities and their suppliers can interface existing investments.

## Functionality

Assigning, suspending and revoking Level 2 user accounts to identity verified individuals

To include a record of the off system identity verification procedure followed, with full auditable history of all changes.

Ideally the system would permit agencies using the system to transfer and import real world user identity verification information from and to other agencies using the system.

Assigning, suspending, revoking and replacing 2-factor tokens with full asset management capability for the whole lifecycle of the 2-factor tokens.

Retrieving authorisation requirements from level 2 access enabled business applications, in order to assign user access rights to that application.

Registering and revoking level 2 user accounts on those applications. Assigning, modifying, suspending and revoking specific access rights to the services and information provided by those applications.

## Appendix A

Answers received from Local Authority Practitioners to a standard set of questions

### For ContactPoint in particular ...

Q. What type of Local Authorities is this relevant for ( i.e. District / County / Unitary / ... and so on )?

- A. As far as I am aware ContactPoint should be available to anyone working with children and / or processing information relating to children.
  
- A. Having discussed this with our Chief Executive, the District Council does not often get involved with Children on an operational basis. The District does deal with Housing, ASBO(s), Leisure, but the volumes are not likely to make changes to our procedures attractive.

#### **Conclusion.**

**The Business Case for adoption by District Councils may be unattractive, as it will only affect a handful of staff. For all other types of Council, this is core business.**

Q. What type of entities ( organisations / partnerships / private sector ) might require that their staff are able to access this information on behalf of a Local Authority, other than direct employees of a Local Authority?

A. This needs to include ALL children's services practitioners not covered by other authentication engines (eg N3, CJIT etc.)

In Leeds this includes our key partners - Education Leeds, Careers Company etc - as well as the numerous Voluntary and Faith sector organisations.

A. The Children's Board in St Helens comprises the local Council, Acute and PCT Health, schools, Connexions, the voluntary sector such as Barnardos etc

#### **Conclusion**

**Authorised access is required by staff other than those directly employed by a Local Authority. Other organisations may not be connected into GCSx.**

Q. How may staff, per Council, typically, would require access to the ContactPoint information and services?

A. In Leeds this could be 3,000+ practitioners - up to 10,000 across West Yorkshire.

A. In St Helens we estimate that 1300 people will require access to ContactPoint. These are made up as follows

600 council  
700 external

The 600 council staff may or may not be on the HR system this is because we employ agency workers and we also have multi-disciplinary teams such as the Youth Offending Service where staff are seconded in from Health, Probation, the Fire Service etc but use our IT services and equipment.

The 700 external users of ContactPoint will be all those not using the Council network and IT facilities, that is schools, Connexions, health, the voluntary sector etc. Some such as Health will have a secure connection.

### **Conclusion**

**For a typical council, this might require that 10% of the staff are authenticated in this way.**

Q. How will a Local Authority determine which staff are empowered to represent it and therefore have the rights to access the ContactPoint information?

A. Council staff will be nominated by their manager as having a need to use ContactPoint. This will also be true of other agencies but the Council **will actually act as the authorising body.**

### **Conclusion.**

**Local Authority employees will be explicitly identified as requiring access to a process, by a Council's Line Management. The notion of 'Roles' does not seem to add value.**

**Where an organisation is empowered to represent a Local Authority, it is not clear if the Local Authority will give explicit rights to each individual, or if the empowered organisation will do that.**

Q How many suppliers of relevant 'Case Management Systems' are there, and how are these being engaged?

A. The Council use OLM's Carefirst as its Social Care Case Management System and Capita EMS for education data. It is currently procuring a piece of software which will act as a portal to all the Children's services applications.

The DCSF are providing uploads of data from the Department and local authorities will be responsible for data uploads from local authority and partner systems. It is possible that the DCSF will also obtain data from the likes of Health, Connexions and other organisations but this has yet to be confirmed.

Q. [How is the current ContactPoint enablement of CMSs taking into account this Level 2 authentication facility?](#)

### **Conclusion**

**Individual Local Authorities are being invited by the DCSF to champion the development of each existing Case Management product, to support the**

**needs of ContactPoint. These Local Authorities should be facilitated to exchange requirements with the CoP group, about**

- Standards, Formats
- Interfaces
- Access to Test Facilities

Q. will access to ContactPoint information be provided using channels other than the web? ( e.g. phone ). How will these channels be authenticated?

### **Conclusion**

**It is unclear how a 'mediator' will determine if a person has the right to access ContactPoint information.**

Q. might Local Government officers require immediate access to ContactPoint information away from their desks? I.e. Mobile Working, Working from Home?

A. Children's Services practitioners are mainly mobile and would want to use the various mobile devices with which they have been issued. However the development may need to concentrate on networked devices initially.

A. Yes

### **Conclusion**

**Unclear how a 'mediator' will determine if a person has the right to access ContactPoint information.**

Q. Given that ContactPoint requires a Level-2 credential ( something that you know, and something that you have ), there may be a requirement for a 'reader' of some sort attached to a device ( PC ). Do we have an expectation of what this might be?

A. All the discussions within ContactPoint to date have suggested the use of Vasco Tokens which would not require a reader. How does this square with the determination of the Health Service to use Smartcards?

A. It is understood that Tokens are to be supplied by DCSF

### **Conclusion**

**Some expectations have already been given to Local Authorities, regarding the nature and source of 'level-2' tokens.**

Q. What lead-in preparations will Local Authorities need to make, and how long might these take?

A. This is one of the crucial issues for Las

What will it mean in terms of administrating the vetting process and how would they popular the GC authentication engine?

What would be the ongoing business process for keeping authentication up to date?

Will ContactPoint be providing a practitioner database to monitor CRB checks and training requirements before a practitioner is registered or will LAs need to develop their own?

### **Conclusion**

**Successful deployment of Contact Point depends other deliverables and progress being made outside of the scope of this Working Group.**

**The project needs to be communicating now to Local Authorities.**

Q How will the proper use of the ContactPoint information be assured, once it has been accessed? I.e. Will those accessing it be required to sign-up to conforming to a code of conduct about the onward use of the information?

A. All agencies signing up to use ContactPoint should have policies in place which embrace the issues raised by ContactPoint. These could include staff training, adherence to Data Protection and Caldicott Principles etc

### **Conclusion**

**A 'model' set of policies will need to be developed to cover the use, storage and onward distribution of information provided by ContactPoint.**

Q. If this project is not able to deliver a credible solution in the required timescale, what fall-back position(s) would be acceptable?

### **Conclusion**

**A fall-back position for providing access to ContactPoint information, should be developed in parallel.**

Q. What are the implications for a failure of these facilities ( e.g. Access given where it should not have been, Access denied when it should not have been). Who is liable for such a failure, and what is the extent of that liability?

### **Conclusion**

## For Employee Authentication in particular ...

Q. What other Government initiatives are we aware of that will require that Local Authority staff are authenticated to access information or transact? E.g. Health - Single Assessment Protocol, Common Assessment Framework. Do we know what the proposals are for how these are to operate? Is there any overlap?

A. **With the announcement of a National E-caf System there is an obvious opportunity to**

try and include their requirements which have being documented for some time! The other potential initiatives around children would be the

Integrated Children's System

Client Caseload Information System (CCIS).

## Conclusion

**Local Authorities will want to have a single approach to**

- **Verifying the Identity of those that represent them**
- **Issuing a credential associated to a verified identity**
- **Managing the life-cycle of an issued credential**
- **Associating further attributes to a verified identity**
- **Enrolling a verified identity to be able to carry out a specified process**
- **Challenging for authentication**
- **Authorising access to information or a service**

**There are a number of current initiatives that are sponsored by Central Government, that will require that Local Authority staff are authorised to access information or services. There is the potential that these solutions will not converge to be a single set of processes and technologies. This 'landscape' should be mapped so that ...**

- A consistent and confident message is given to Local Authorities
- Convergence of processes and technologies is a design goal.

Q. What procedures and technologies have Local Authorities typically implemented already to provide Single Sign-on to their staff?

A. None

## Conclusion

Local Authorities are at various stages of roll out of local implementations of Single Signon.

Q. Is there an expectation that Government Departments , will want to access information held and controlled by a Local Authority?

A. Not aware of any at this time

## Conclusion

**The 'mapping' of other initiatives should establish if information is to 'flow' the other way, such that Central Government departments are able to access Information and Services from individual Local Authorities.**

Q. Is there an expectation that Non-Local Authority staff will be required to represent a Local Authority. E.g. Outsourced data processing, shared customer services and so on. If so, who will be liable for the ....

A. Yes. Ultimately the LAs is responsible for its own area.

A. Yes

## Conclusion

**Local Authorities will verify the identity of its own directly employed staff. For staff from other organisations who are empowered to represent a Local Authority, either**

- **The Local Authority will perform the Identity Verification process.**
- **The empowered organisation will perform the Identity Verification.**

**An employee of a non local authority organisation may be empowered to represent more than one Local Authority.**

Q. To what rigour do Local Authorities currently typically verify the identity of their staff, and further attributes such as clearances and qualifications?

A. **very variable amongst all partners and within the Local Authorities.**

A. This is the response from our HR department about staff checking. This is the basic check on entering employment, however, staff employed before this came into force were checked but not with the same rigour. Should the employee be working with vulnerable clients or accessing ContactPoint (this may be optional) then further checks such as CRB enhanced are also carried out. Under Section 12 of the Children Act these must be repeated every 3 years.

‘The Asylum and Immigration Act 1996 makes it a criminal offence to employ someone who does not have the right to work within the UK. Regulations introduced from 1 May 2004 under the powers in the Act changed the documentation that employers are required to check to confirm this. This documentation, even at the most minimum level, would meet that identified in item 1 of the BS checks described, and also by default that in item 4.

The only possible issue would be whether or not the employees involved commenced before this was introduced, however, even in those circumstances their identity would have been confirmed by provision of a P45, National Insurance Number, birth certificate, etc. Their nationality and immigration status would not have been verified in the same way as now.

In respect of the other two items:

- employment history (past 3 years) - managers should be checking gaps in employment histories provided at interview. The most recent employment is also checked via the requirement to list the most recent employer as a referee.
- similarly even our basic application forms, used for many years, have asked candidates to self declare any unspent convictions that they may have. This, therefore, should meet the standard required. The enhanced application form, which may not be applicable to these posts, goes beyond this and requires that all convictions be declared.’

## Conclusion

**A single ‘Identity Verification and Registration’ process will be required across all organisations that register staff.**

**This will require negotiation across the Local Government Community.**

**The 'information or Service owner' will prescribe the pre-requisites for access. Therefore, a minimum acceptable registration process will be required to be adopted across the Public Sector.**

Q. if any Government Connect product, is to be deployed within the Trust Domain of a Local Authority, what are the risks? , and how might they be mitigated?

A. Especially if the authentication engine is not available for any reason! Will this be a central engine or regional/sub-regional engines?

There will be a need for useable back office APIs to enable SSO to work - how and when will this be built into the timeframe?

### **Conclusions**

**Concern about the dependency and resilience on externally provided facilities that might impact on a Local Authority's ability to carry out its duties.**

**Service Levels should be defined.**

**A Risk Assessment of the need for resilience should be undertaken.**

**A 'fall-back' position should be established to 'kick-in' should these facilities fail.**

### **Further comments received from Local Authorities.**

We need a solution that enables transactions between local authorities and central government and other public sector bodies e.g. NHS.

We need to know how much this will cost per user and ongoing annual maintenance costs.

We need to know what standards, if any, we need to apply in order to have access such as a code of connection. We need to have a standard code of connection across domains - it would seem bizarre to have to do one thing for Gov Connect and another for ContactPoint.

We need to know realistic timescales for delivery - so that we can include within our project/programme plans.

We need a solution that meets our requirements but does not conflict with existing security solutions and user management tools.

Salford City Council is an early adopter of ContactPoint - this means we need to know what solutions will be available for our deployment slot (currently April 08) and the timeline for other solutions coming online so we can make decisions about whether for example, we register a minimum of users to ContactPoint's own domain in the first instance in the knowledge that 6 months down the line we would be moving to an alternate domain or whether it will be 24 months until there is a wider solution and hence we might register all our CP users against CP's own domain.

Salford City Council's user base does not comprise solely of employees but also of agents acting on behalf of the council or, as in the case of CP, users for whom Salford City Council is responsible for registering because these users fall within Salford City Council's geographical

boundaries. These users have diverse requirements and so it is expected that the following will apply:

1. 2 factor authentication - hardware - there will be a multiplicity of hardware tokens depending on the requirements of the user - we would require the flexibility to decide which token for which user
2. Access will not be granted based on job title - not all social workers will access CP for example
3. We would want standardised messaging (e.g. defined xml schemas preferably govtalk) for user movement - new starter, suspend, leaver, termination etc.

A level 2 authentication system is required to allow staff undertaking their employer's official business activities electronic access to IT applications transacting, personal, confidential, sensitive or restricted information.

These IT systems may be operated by any provider, directly, or under contract, i.e.

- Central Government Departments (CG)
- Local Authorities (LA)
- Commercial Suppliers (CS)
- 3<sup>rd</sup> Sector Organisations (3S)

The system should allow authenticated and authorised transactions conducting Local or Central Government business in any direction, i.e.

- CG to CG, CG to LA, CG to CS, CG to 3S
- LA to LA, LA to CG, LA to CS, LA to 3S
- CS to CG, CS to LA, CS to 3S
- 3S to CG, 3S to LA, 3S to CS

if a need for CS to CS, and 3S to 3S transactions is established the system should also be capable of supporting them.

In order to deliver a workable, practical, affordable, and efficient system the requirement is therefore for a single solution for all staff:

- directly employed by Local Authorities
- working under contract to Local Authorities
- secondees, employed by other agencies but working in Local Authorities
- working for 3<sup>rd</sup> sector agencies (Voluntary organisations, Not for Profit Organisations) under contract to Local Authorities
- working for commercial service suppliers under contract to Local Authorities (outsourced functions).

The functions required:

1. A nationally agreed set of Identity Verification procedures (for confirming the real world identity of the individual requiring Level 2 authentication).

2. A computerised application for:
  - a. Assigning, suspending and revoking Level 2 user accounts to identity verified individuals
    - 
    - i. To include a record of the off system identity verification procedure followed, with full auditable history of all changes.
    - ii. Ideally the system would permit agencies using the system to transfer and import real world user identity verification information from and to other agencies using the system.
  - b. Assigning, suspending, revoking and replacing 2<sup>nd</sup> factor tokens with full asset management capability for the whole lifecycle of the 2<sup>nd</sup> factor tokens.
    - i. Retrieving authorisation requirements from level 2 access enabled business applications, in order to assign user access rights to that application.
    - ii. Registering and revoking level 2 user accounts on those applications.
    - iii. Assigning, modifying, suspending and revoking specific access rights to the services and information provided by those applications.

## Appendix B

Central to Local Government Initiatives requiring authenticated access to information or processes.

Project	Sponsor	Overview
ContactPoint	Every Child Matters  DCSF	<p>the quick way for a practitioner to find out who else is working with the same child or young person, making it easier to deliver more coordinated support.</p> <p>Authorised users will be able to access ContactPoint in three ways - through:</p> <ul style="list-style-type: none"> <li>• A secure web link</li> <li>• Some existing case management systems</li> <li>• Another authorised user (where appropriate IT is unavailable)</li> </ul> <p>Wherever possible ContactPoint will be automatically updated from existing systems, avoiding the need for practitioners to enter information on a separate system. It will not be possible for an authorised user to access case management systems or to see case data held by another agency on ContactPoint.</p> <ul style="list-style-type: none"> <li>• Access to be restricted to those who need it as part of their work.</li> <li>• Everyone with access to be subject to stringent security checks, including enhanced Criminal Records Bureau clearance.</li> <li>• A minimum of 'two-factor' authentication will be required for access.</li> <li>• All users will be trained in the importance of good security practice.</li> <li>• Users must be able to state a reason for accessing a record.</li> <li>• Every access to a child's record will be detailed in the audit trail. This will be regularly reviewed to ensure that any misuse will be detected.</li> <li>• Various sanctions will be available to tackle misuse, including disciplinary action or prosecution under existing legislation, which may result in a fine or imprisonment.</li> </ul>
Client Caseload Information System	Every Child Matters  DCSF	<p>The Client Caseload Information System holds a range of information on young people aged 13-19 in order to assess progress in local areas on a range of measures, including cutting the number of young people not in education, employment or training (NEET). The system is currently run by Connexions partnerships. From 2008 local authorities will be responsible for delivering the Connexions service.</p> <p>The information held on the system about young people</p>

		<p>includes data on the:</p> <ul style="list-style-type: none"> <li>• Young person's needs</li> <li>• Current levels of attainment</li> <li>• Intended destination on leaving school</li> <li>• Details of any other agency working with the young person</li> </ul> <p>All lead professionals in the area working with young people can be given access to their local Client Caseload Information System. This is strictly controlled through role based security and only with consent of the young person. The system can also support ContactPoint by providing basic up-to-date information on young people.</p>
Integrated Children's System	<p>Every Child Matters</p> <p>DCSF</p>	<p>The Integrated Children's System (ICS) is a framework for working with children in need and their families.</p> <p>to be supported by an electronic case record system. A key aim of ICS is to provide frontline staff and their managers with the necessary help, through information communication technology (ICT), to record, collate, analyse and output the information required.</p> <p>Each local authority is required to produce its own solution for ICS that delivers the business requirements set out in the local authority circular LAC(2005)3, making use of guidance documents that address practice, core information requirements, ICT functionality, information outputs and the learning from pilots.</p>
Customer Information System ( CIS )	DWP	
Information Flows	DWP	
Informaiton Management Programme	CLG	
Crime and Disorder. Exchanging Information	Home-Office, Police, CJ	