Australian Government

Digital Transformation Office

National e-Authentication Framework

Better Practice Guidelines – Vol 3 Implementation Models

January 2009

Disclaimer

This document has been prepared by the Department of Finance and Deregulation (Finance) to provide information to government bodies in relation to the use of e-Authentication for government transactions.

While every effort has been made to ensure that the document is accurate, no warranty, guarantee or undertaking is given regarding the accuracy, completeness or currency of the document. This document should not be relied upon as legal advice. Users are encouraged to seek independent advice relevant to their own circumstances.

Links to other websites are inserted for convenience only and do not constitute endorsement of material at those sites, or any associated organisation, product or service.

ISBN 0 9758173 7 X

Department of Finance and Deregulation
Australian Government Information Management Office

Acknowledgements

Photographs taken by Steve Keough, Steve Keough Photography

Contents

Figures

Tables

1. Introduction

The National e-Authentication Framework (NeAF) recognises and accommodates sectoral and whole of government initiatives through the re-use of existing authentication credentials and consideration of a variety of identity management frameworks as alternatives to traditional agency specific models.

The ongoing application of the NeAF across government agencies will result in the alignment of e-Authentication approaches within government agencies and applications across Australia. Across participating agencies this will provide consistency of:

- the determination of application assurance needs and associated authentication risk mitigation approaches
- implementation of end user identification and registration, and credential provisioning processes, for various assurance levels across both agencies and user segments; and
- selection and utilisation of various e-authentication credentials and e-Authentication mechanisms for various assurance levels as required by application systems.

Consistency of approach and implementation will create opportunities for cross agency e-Authentication. Such schemes will provide more convenient e-Authentication approaches to citizens and businesses, and more effective utilisation of resources by participating agencies.

This e-Authentication Better Practice Guidelines has been written as a guidance document and describes a number of internationally recognised authentication models and the associated issues that should be addressed. Because e-Authentication is considered fundamental to ensuring trust and confidence in online transactions between government and business and individuals, agencies need to be aware and implement appropriate e-Authentication strategies.

The objectives of this document are to provide agencies with:

- direction and support on e-authentication (and associated) models and approaches; and
- guidance on issues that agencies should address when implementing e-Authentication.

It will be important to consider which implementation model/s should be adopted when undertaking the development of an agency e-Authentication strategy (see Better Practice Guidelines Volume 4) and when designing the e-authentication for a transaction or cluster of transactions (see Better Practice Guide Volume 1).

This document is currently under review by the Digital Transformation Office.

2. Current and Emerging Implementation Contexts and Service Delivery Models

Service Delivery Models are models of the business processes used to deliver services to clients.

Early implementations of electronic service delivery were based around specific agency requirements with each implementation self contained functionally, technically and operationally. This is referred to as the Siloed Delivery Model. Whilst still functional and still in widespread use, the Siloed Delivery Model is being displaced by models offering improved efficiency and usability.

The emergent service delivery models described in section Service Delivery Models are aimed at:

1. improving the efficiency of electronic government services delivery through reuse of core infrastructure
2. decreasing users' need for awareness of the distribution of various business service delivery facilities across government agencies, and changes in this distribution over time through machinery of government changes
3. enabling increased user centricity – allowing users greater choice in how they deal with government – e.g. reducing the number of e-Authentication credentials they choose to hold; and
4. retaining, and potentially enhancing, agencies' abilities to implement a risk based approach to user authentication.

2.1 Service Delivery Models

The service delivery models can be described as:

2.1.1 Sectoral (national and jurisdictional)

In a sectoral model, participants offer sector-specific services across a range of agency, jurisdictional and potentially private-public sector boundaries to provide end users seamless access to sector specific services. Examples exist in health, education, law enforcement, emergency services.

EXAMPLE

1. The proposed National E-Health Transition Authority (NEHTA) National e-Authentication Service for Health (NASH).

2.1.2 Whole of government (portals for citizens and businesses)

In a portal model governments offer one or more common access points (portals) to a range of government services. The intention is to allow users to readily access services largely transparently of which agency hosts the services and across various government agencies.

EXAMPLES

1. The proposed Australian Government Online Service Point (AGOSP) single sign-on service.
2. Service Tasmania and the one-stop government services point in remote communities are real world examples of this service delivery model.
3. New York City's 311 Service is an example of this service delivery model applied to a 'telephonic' world.

This document is currently under review by the Digital Transformation Office.

2.1.3 Agency clusters

In an agency cluster model, agencies with similar user bases provide portal based access and potentially work together to create a number of linked and interdependent workflows to support end user information or transactional needs.

EXAMPLES

1. the Australian Government's Human Services (DHS) portal
2. the Victorian Government CJEP system which links Police, Courts, and Corrections systems to provide a single application perspective.

This document is currently under review by the Digital Transformation Office.

3. Authentication Models

The following sections provide information and implementation guidance on a number of identity e-Authentication implementation models that can support the above electronic service delivery models.

Each of the authentication implementation models described comprise the elements of the baseline implementation model outlined in section Baseline Functional Model and Concepts, however the distribution of functionality and accountability for these elements is different for each model.

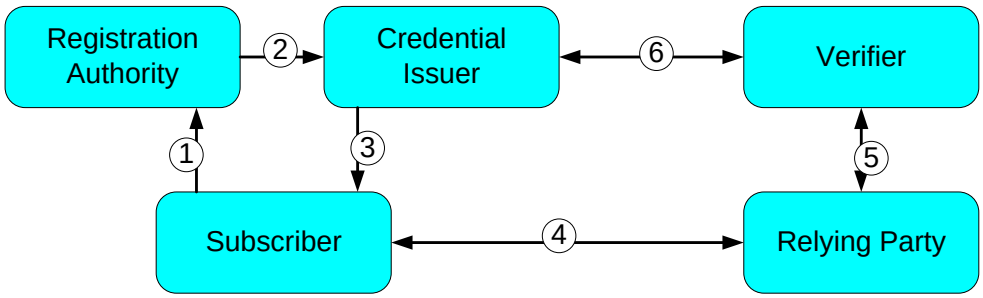
3.1 Baseline Functional Model and Concepts

3.1.1 Model Components

The baseline functional model depicted in Figure 1 outlines the common events and steps in lifecycle management for most authentication systems – from registration, through to credential issuance and usage by the subscriber.

Whilst each of the identity authentication implementation models described later in section 3.3 implement the elements of the baseline functional model, the distribution of functionality and accountability for these elements is different for each implementation model.

Figure 1: Baseline Functional Model



This model addresses the full credential issuance and usage lifecycle including identity proofing, credential issuance, credential verification and ongoing management of active credentials as described within the NeAF.

Definitions of the terms and roles in the model above are contained in the Glossary of Terms.

The baseline functional model described above can be implemented in a variety of ways. Silo implementation models result in the agency implementing all roles, whereas other models result in the various roles and underpinning functions being distributed across agencies and service providers.

3.1.2 Model Concepts

The distinction between registration and enrolment is particularly important to an understanding of the differences between e-Authentication Implementation Models. Figure 1 – Identity and Access

This document is currently under review by the Digital Transformation Office.

Management Lifecycle (showing information stores) – in Better Practice Guidelines Volume 4 illustrates the difference between registration and enrolment[1].

In the NeAF context:

- Registration represents the processes associated with the initial creation of an electronic identity for a user. Registration usually encompasses EOI (evidence of identity) and/or EOR (evidence of relationship) processes.
- Enrolment is the act of binding an e authentication credential to a known instance of a user within an IT resource context (e.g. network, website, application system) in order to enable access by the user.

See section 4 (Framework Methodology) of the Framework, and Better Practice Guidelines Volume 1 for a detailed examination of the above particularly in relation to *known* and *unknown* customers.

3.2 Identity Authentication Implementation Model Components

The following section describes the major building blocks, including functions and organisational context, which must be addressed within most identity authentication implementation models.

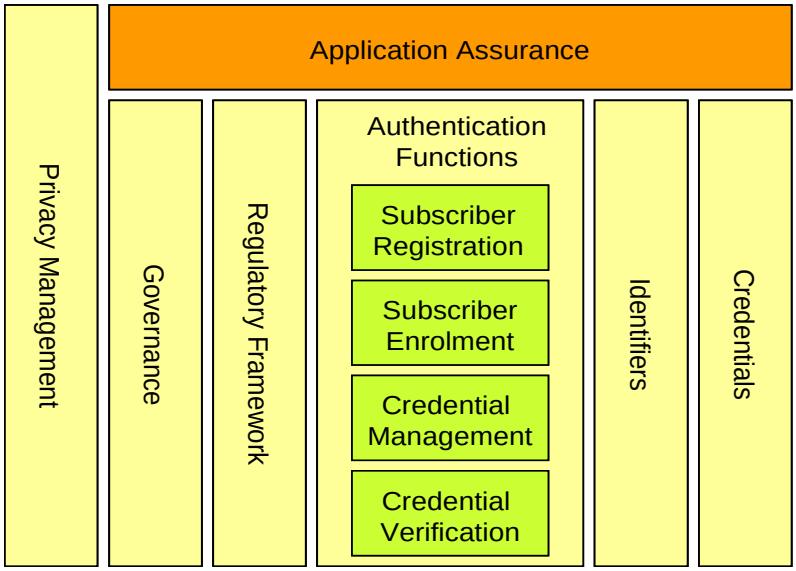
Contemporary identity authentication implementation models are described by and differentiated by a range of factors including:

- the distribution of the authentication related roles and functions (described below) across the various operating participants
- the treatment of identifiers within the models and the related privacy implications and controls. For example, some models mandate the use of a single identifier linked to the authentication credential to be used for access to all applications and agencies, whereas other models enable discrete application or agency specific identifiers to be linked to a credential; and
- the legal frameworks and governance regimes which underpin the models. These will result in varying degrees of authentication assurance, and specify avenues for recourse available in the event of authentication errors.

These factors and their interrelationship are presented in Figure 2 below.

[1] The difference in the usage of this terminology within key Australian Government policies is also important to understand. See the discussion of NISS and GSEF in Appendix 1-Risk and Security Policies and Standards of the Better Practice Guidelines – Volume 4.

Figure 2: Authentication Implementation Model Components



Most implementation models are, in themselves, independent of the credentials that are deployed within the model, although some models are more suited to particular credential types. Nonetheless credentials are a core component of any implementation model, being the visual output of the model.

3.2.1 Identity Authentication Functions

The following major functions are implemented within identity authentication models:

1. Application Assurance Level Determination

The NeAF contributes to the achievement of the objectives of the e-Government Strategy by facilitating a consistent approach by agencies across all tiers of government to the management of unacceptable identity-related risks for the purpose of facilitating secure and easy interaction with government. It will guide agencies in determining:

- the level of authentication required; and
- an e-Authentication solution approach that will enable end users to build trust and confidence in electronic transactions with government.

As described within the NeAF the assurance level determines the strength of identity authentication required based on an assessment of the risk of interactions with their end users (i.e. businesses or individuals).

This task is relevant to authentication model selection because it is the major driver for the existence of e-authentication services, and because consistency in determination of assurance levels is important across organisations seeking to ‘share’ authentication credentials.

2. Subscriber Registration

Subscriber registration includes:

- the identity proofing of subscribers to a determined assurance level as described within NeAF
- the allocation or assignment of an identifier to the subscriber for use in electronic dealings with relying parties; and
- in some implementation models, the registration process would instigate the issuance of a credential to the subscriber.

3. Subscriber Enrolment

The act of enrolment is a key distinguishing feature of non-silo-based models and is therefore given an extended treatment in this section.

Enrolment involves the binding of an existing (i.e. already registered or "known") subscriber instance within an agency to a credential that has been issued to the subscriber by a third party. Enrolment is a major construct of federated identity regimes which enables third party credentials to be linked to an existing subscriber account within an agency for later use in authentication of that subscriber.

In some implementation models this binding or linkage is implicit to the issuance of a credential to a subscriber as a flow-on function to registration. In other implementation models this binding is initiated by the subscriber through an enrolment process offered by the relying party. This method of linkage of a previously issued credential to a known user is a fundamental element of the Australian Government Online Service Point (AGOSP) single sign-on portal and the DHS authentication hub.

The enrolment process requires agencies to:

- **Satisfy themselves that the presented credential is of a suitable assurance level.**
- **Have access to the credential issuer so that the agency can validate a credential presented by the subscriber as part of an enrolment process.** This could involve, for example, the validation of a One Time Password (OTP) or verification of a signature generated from a smart card. Alternatively, it might require the validation of an assertion presented by an authentication gateway or hub, as is the case with AGOSP or VANguard.
- **Complete a validation of the identity of the requesting subscriber in the context of the agency's application system.** This validation may be completed online, or in person or by a combined approach. Online enrolment would typically involve challenging the subscriber to provide information shared by the agency and the subscriber in order to satisfy the agency that the enrolling subscriber is who they purport to be. This information could relate to specific prior dealings between the agency and the subscriber, but could also include specific user determined secrets provided by the subscriber at initial registration with the agency.

The nature of the validation (that the subscriber is who they claim to be) process is a matter for the agency to determine. As enrolment is specific to each relying party there is no systemic risk introduced by the agency's enrolment process – the risks are agency specific.

Notwithstanding the above, the enrolling agency should apply equivalent identity validation steps to the binding process as to the initial subscriber registration within the agency for the target NeAF assurance level.

- **Bind the agency records to the credential.** This might be completed by the storage of a credential identifier in the agency's customer database or Identity and Access Management directory for subsequent use by the agency in credential validation.

In a federated environment this binding may be implemented through the storage of a persistent pseudonym within the customer database which would thereafter be included, by the authentication gateway, in identity assertions relayed to the agency.

4. Credential Issuance and Management

Credential issuance involves the authorised generation and issuance of an authentication credential and the assured activation of the credential by the subscriber.

Lifecycle management of the credential may include credential re-issue, unblocking of a credential blocked through multiple invalid verification attempts, PIN resetting of device based credentials, suspension of credentials, and revoking and cancelling of lost or stolen credentials.

As many of the management obligations are in response to subscriber requests (PIN reset, lost credential etc), the credential issuer must maintain mechanisms to validate these requests which may originate through a call centre or through online self service facilities offered by the credential issuer.

The integrity and robustness of credential issuance and management processes are at the heart of high assurance authentication regimes.

4. Credential Verification and Validation

Credential *verification* relates to the verification of the submitted credential as a precursor to enabling the conducting of a transaction. This occurs through e.g. the verification of a password, one time password, signature etc as being correct for the specific credential.

Credential *validation* relates to the status of the credential at the time of verification. States that might result in validation failure include lost credential, suspended credential, expired certificate etc.

The credential issuer is the authoritative source of credential validity. In order to verify and validate a subscriber authentication request, a relying party requires direct or indirect connection to the credential issuer. In some cases indirect connection might be provided by an intermediary acting as a “trust broker”.

Verification and validation of credentials can be achieved through a range of information flows between relying parties, credential issuers, verifiers and intermediaries, and these are described in later sections.

4.1 Identifier Usage

Increasingly, authentication models are seeking to provide privacy-aware completion of authentication. These models seek to enable subscribers to utilise the same credential for interactions with many relying parties, without a single point of aggregation of information. This prevents the joining-up of a subscriber’s dealings across relying parties.

Authentication models implemented by the Canadian and New Zealand governments have implemented privacy-aware techniques as core elements of their authentication models. Both models have adopted what are essentially anonymous credentials that are issued and managed by a trusted credential issuer but are not backed by any subscriber registration process. Instead, the binding of the trusted credential to the subscriber’s identity is completed as part of an enrolment process as described above.

A common identifier is neither maintained across nor available to participating relying parties.

Moreover, the subscriber is in full control of which credential (of potentially a number they may possess), that they use for specific authentication purposes.

The assurance level assigned to these credentials in each agency’s context will be dependent upon the strength of the underpinning authentication mechanism, and the nature and strength of the agency’s enrolment process as described above.

4.2 Governance and Regulation

Governance

Authentication models typically exist within a governance regime that monitors participants’ compliance with various obligations and potentially regulations and directs strategy for the ongoing development of the services offered.

As parts of the authentication process are external to an agency, the agency increasingly relies upon others for execution of its risk management measures.

Agencies that currently rely upon certificates issued by Gatekeeper accredited Certification Authorities for authentication of their subscribers have the assurance of a robust externally managed accreditation and ongoing audit program to ensure the integrity of these outsourced credential issuance and management functions.

Regulatory Framework

Authentication models that support high assurance authentication should operate within a regulated framework. This is most important in a federated model where the responsibilities and accountabilities associated with operations are usually spread over a number of distinct legal entities.

Areas that are typically addressed within the regulations are registration and issuance processes, credential characteristics (key lengths, PIN policies, etc), dispute resolution processes, assignment and resolution of liabilities, performance and availability requirements, operational processes, technology standards and subscriber interfaces.

Authentication models that support lower assurance authentication would likely operate with a lighter touch approach that may be underpinned by Memoranda of Understandings or similar instrument between the participants.

This document is currently under review by the Digital Transformation Office.

5. Identity Authentication Implementation Models Descriptions

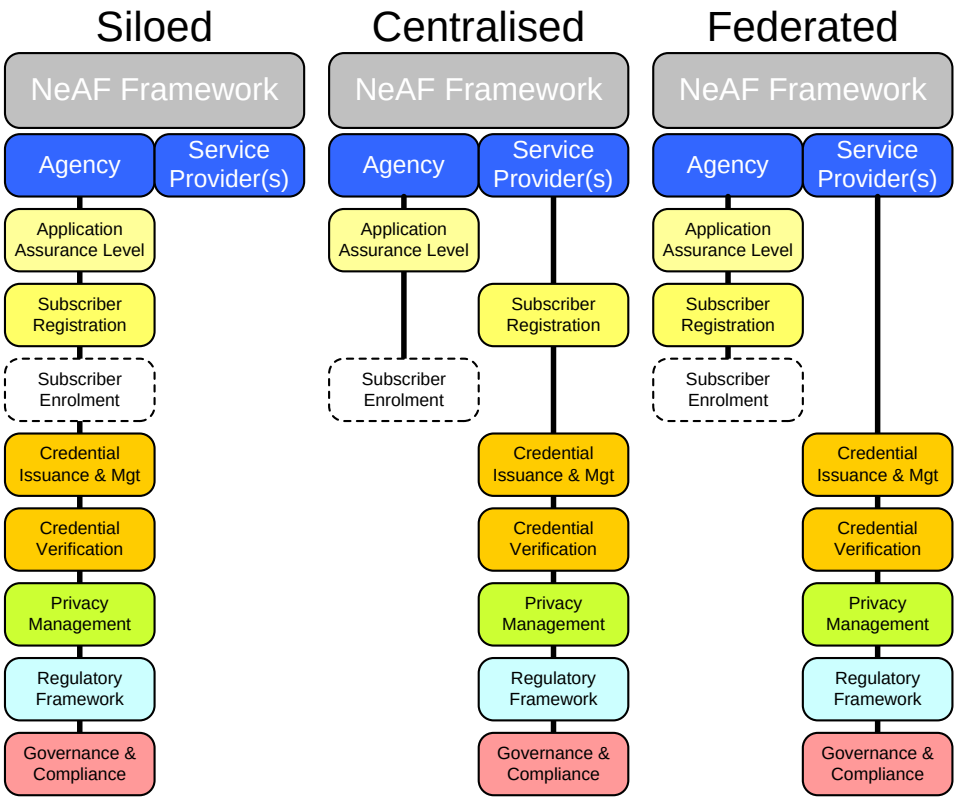
The authentication models discussed in this section are implementations of the baseline functional model set out in Figure 1. Each of the authentication models vary in how key functions (in the functional model) are distributed between agencies (as relying parties) and service providers.

Note – service providers may be other agencies or private sector service providers as is the case with some Gatekeeper accredited providers.

For example, in the context of AGOSP, AGIMO is a service provider to relying parties (other agencies), providing credential issuance, management and verification services.

Figure 3 below illustrates the siloed, centralised and federated authentication implementation models. These models are further described in the following sections.

Figure 3: Authentication Models – Functional Distribution



Within the diagram, functional areas fall under either agency or service provider/s headings, with potentially multiple service providers fulfilling distinct roles.

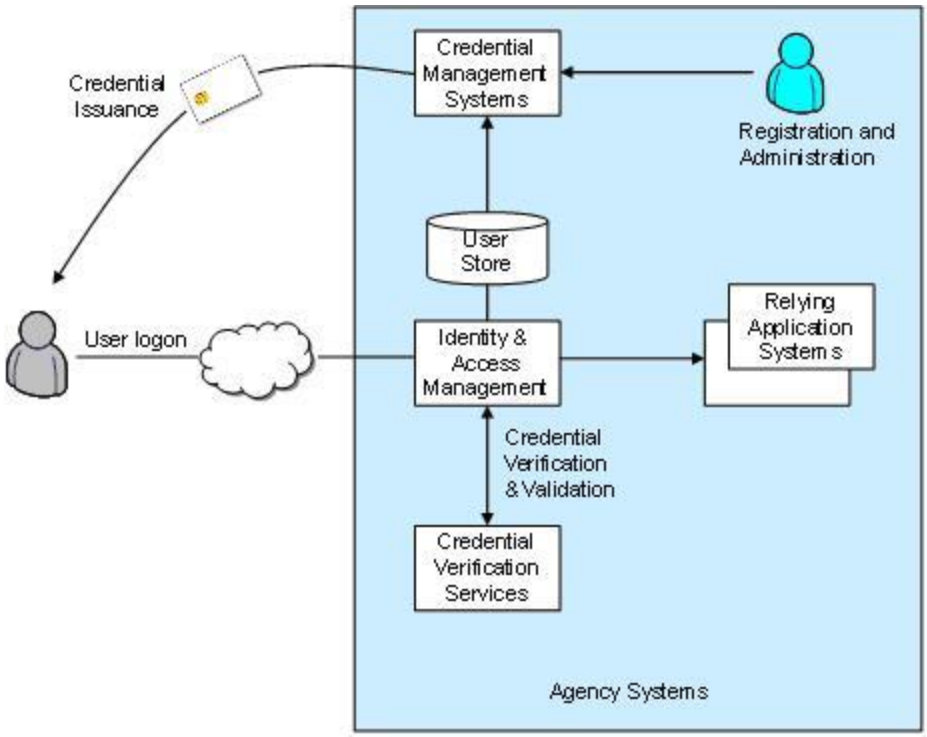
Note: It is possible for agencies implementing a *siloed* model to utilise service provider facilities similar to those provided under a *centralised* model.

5.1 Siloed Model

This authentication model is fully implemented and managed by an agency (or application in many cases) and does not implicitly support broader use of subscriber credentials, or subscriber registration assets across other agencies. It may, as noted above, make use of 'outsourced' services and facilities.

The model is illustrated in Figure 4 below.

Figure 4 Siloed Model



5.2 Centralised Model

This authentication model enables agencies to leverage a well defined user registration and authentication model, implemented by others, for use within agency applications.

A centralised model will typically involve the use of a single credential, with an explicit identifier for the subscriber, for use across all agencies that recognise the centrally issued and managed credentials.

The identifier would generally be either contained within the credential (such as a certificate) or would be provided through an attribute of the credential (such as a token serial number) or a verifiable channel to an associated identifier.

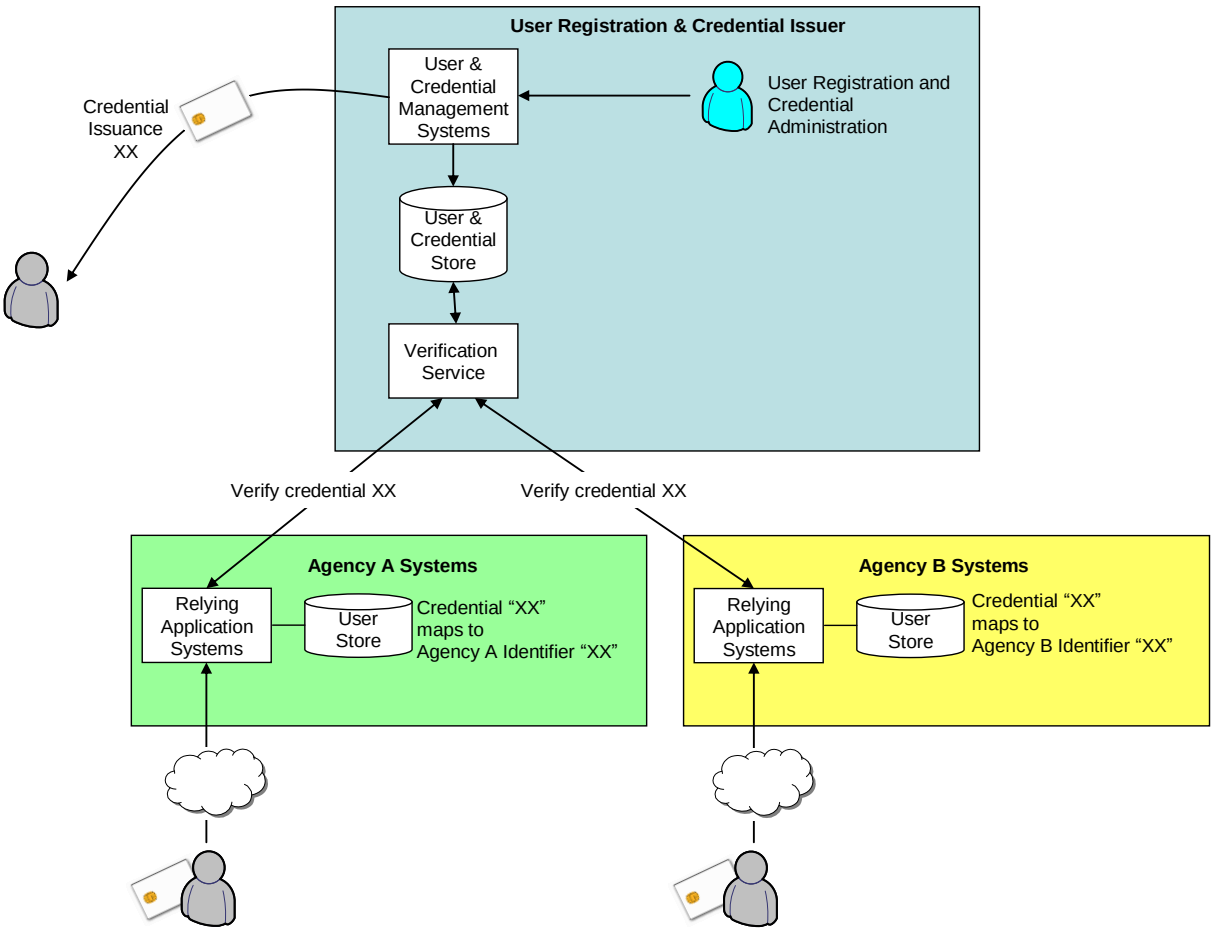
The identifier would relate to a single discoverable identity, established at subscriber registration and as such the enrolment function (shown with dotted outline in Figure 3 above) is implicit to the registration process.

The Gatekeeper General Business Certificate implementations are considered centralised. There are a number of issuers of compliant certificates, however the credentials issued under this program have standard profiles, consistent policies, contain identifying information and generally equivalent assurance level.

This document is currently under review by the Digital Transformation Office.

A centralised model as described above is illustrated in Figure 5 below.

Figure 5 Centralised Model



5.3 Federated Models

Federated identity management is a term that has a range of meanings and interpretations across various vendors, practitioners and commentators.

Wikipedia provides a useful definition being

> *federated identity, or the 'federation' of identity, describes the technologies, standards and use-cases which serve to enable the portability of identity information across otherwise autonomous security domains.*

The term "identity information" in the following discussion is defined as the information required to authenticate the identity of a subscriber across security domains.

In this context, three variations of federated identity authentication models are described below.

In each instance (and unlike the siloed and centralised models), the binding of a subscriber's identity (a function of agency registration) and an associated credential is established through a late binding process completed through the subscriber's enrolment with the agency.

5.3.1 Federated Portal

A federated portal or logon service provides subscribers with a single sign-on service across multiple agencies or independent security domains without requiring the use of a single identifier across these domains.

In this model credentials are issued by a portal service provider after conducting a registration process; a subscriber's actual identity would not necessarily have to be disclosed as part of this e.g. as in AGOSP and the Canadian and New Zealand examples. Credentials issued by this provider can be leveraged by agencies for subscriber authentication after the completion of subscriber enrolment processes which bind the (service provider issued) credential to a registered (i.e. already known) user within the agency.

Agencies (relying parties) remain responsible for their own (original) subscriber registration and enrolment processes to their required assurance levels but rely upon the portal to authenticate the credential of the connecting user. Subscribers must be registered within the agency's systems prior to enrolment.

In this model, participating agencies have no direct access to authentication functions that are implemented within the portal such as verify credential, verify a signature etc. Moreover they have no specific knowledge of the submitted credential (such as credential type), excepting for its assurance level.

Instead, these low level functions are completed by the portal and the outcome communicated to the agency via an authentication assertion that can be validated by the agency.

The portal service provider is responsible for all elements of credential verification and validation, and issuance and management to specified assurance levels. The assurance level in this instance applies to the authentication mechanism only.

The federated portal model will typically result in a subscriber retaining distinct internal agency identifiers within each of the participating agencies. At subscriber enrolment time the portal will assign an internal persistent pseudonymous identifier for subsequent use between the portal and each agency to communicate the authentication status of a subscriber seeking to access the agency's systems.

As a consequence of this, the portal service maintains information that could be used to link subscriber identity information across agencies and as such should be suitably secured.

This model is in use in a number of e-government environments including GLS (Government Logon Service) in New Zealand and the AGOSP Single Sign-on Service.

This model can be implemented to support two authentication flows:

1. Portal logon service

In this flow a user would logon to a portal which would present the user with a logon screen. After successful logon the user would be presented with a view of those (agencies') services available for selection by the user. Upon selection the user would be transferred to that service as an authenticated user.

A generalised depiction of a federated portal implementing the Portal login service flow is shown in Figure 6 below.

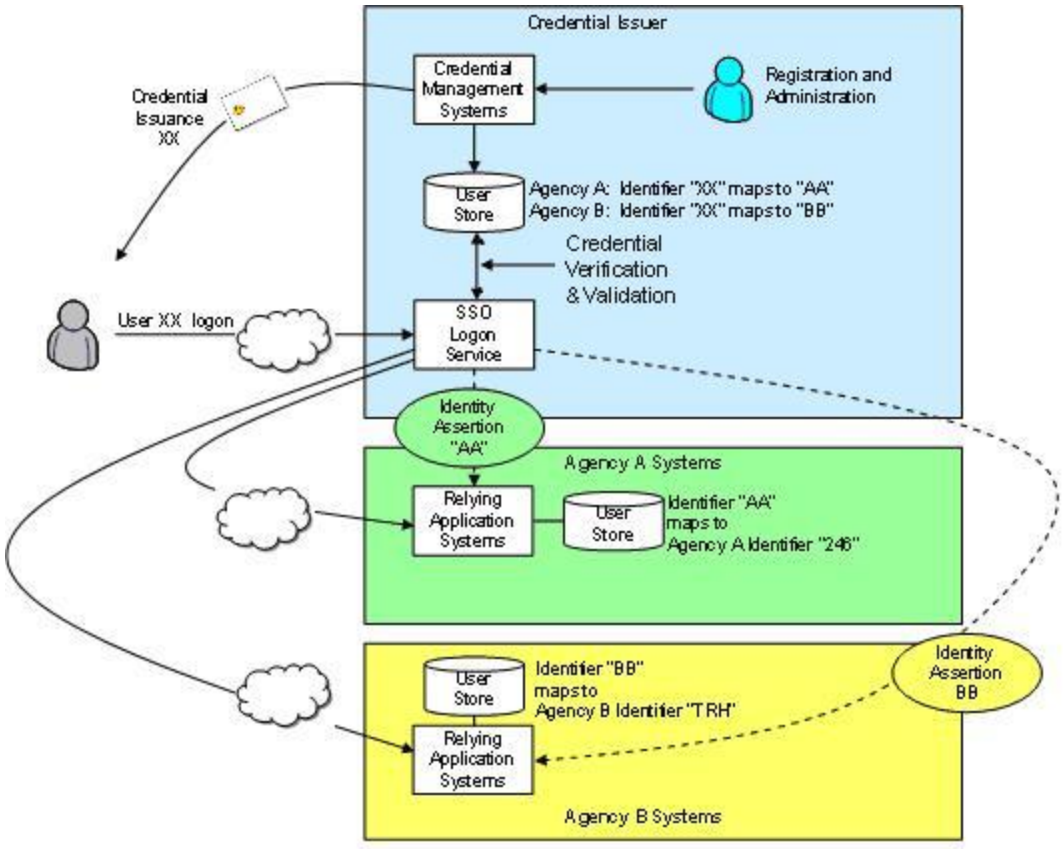
This document is currently under review by the Digital Transformation Office.

2. Agency logon

In this flow a user would logon to an agency's web site. The agency would then redirect the user to the logon service to complete user authentication. Once complete the user would be redirected back to the initial agency web site as an authenticated user.

A federated portal model as described in section Federated Portal above is described below in Figure 6.

Figure 6 Federated Portal



5.3.2 Peer to Peer Portal

This is an extension of a federated portal, whereby participating agencies may act as portal service providers for other agencies.

Responsibilities and accountabilities align closely with the federated portal model, albeit single agencies may be operating as both portal service providers and relying parties.

In peer to peer arrangements it is likely that the governance and regulatory framework would also be implemented bilaterally.

5.3.3 Federated Portal PLUS

Whilst excluded from detailed discussion, this model is an extension of the federated portal and includes the concept of a user managed account, maintained within the portal, within which the user may store various identifying and related information for selective release to agencies under explicit user authority.

This model extends the credential verification role of the portal to potentially include registration support, or in a further extension, to include registration.

New Zealand Government initiatives in Identity Validation Services are examples of this extended functionality.

5.3.4 Federated Authentication Services

Whilst maintaining the concept of reuse of authentication credentials across security domains, the federated authentication services model has no single point of storage of subscriber identity information that would support the aggregation of more general subscriber information across agencies.

Within this model, rather than connecting through a portal logon service, subscribers connect directly to agencies using a credential issued by a credential issuer.

Agencies maintain verification and validation service interfaces to the credential issuer or a verifying agent.

As for the federated portal service described above, a subscriber, already registered with the target agency, presents a credential to the agency, which then refers this credential to the verification point for verification. After verification, the agency binds the credential to the subscriber.

Unlike the federated portal models described above, no information is held outside the agency in respect to this binding.

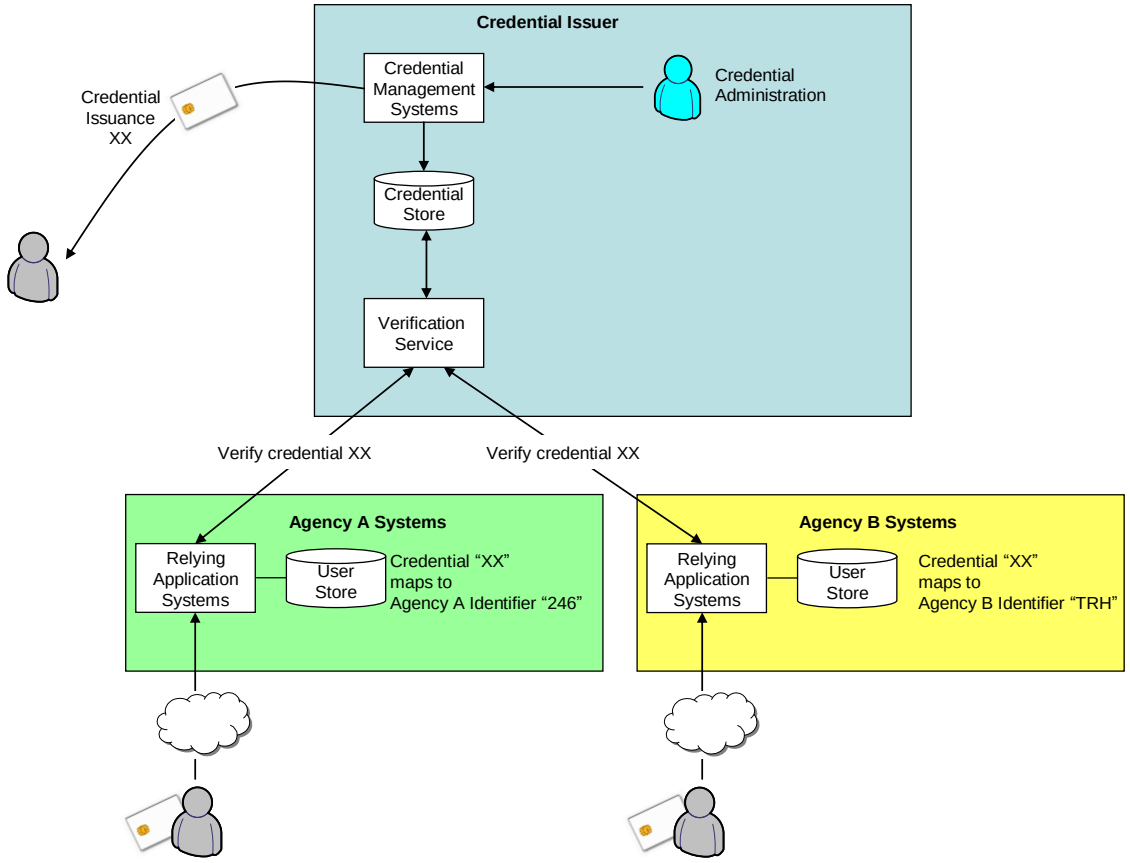
As the agency has direct interaction with the credential issuer, this model is readily extensible to support more sophisticated transaction authentication services that are not typically supported within the authentication portal model.

These could include transaction and document authentication, notary services etc.

A generalised depiction of a federated authentication services model is shown below in Figure 7.

This document is currently under review by the Digital Transformation Office.

Figure 7 Federated Authentication Service Model



This model can be further extended operationally with the introduction of an organisation acting as intermediary between one or more agencies and one or more credential issuers. Organisations providing these intermediary services are often termed "trust brokers".

Trust broker services potentially offer advantages to participating agencies through operational simplicity, in that only one external interface is required for all authentication services, and ease of integration of additional authentication mechanisms as they become available.

The extent to which these advantages apply to individual agencies will be affected by the number of external credential types that the agency seeks to support and the extent to which functions such as audit logging, policy enforcement (e.g. for PKI certificates) can be fully outsourced to the trust broker.

It is emphasised that utilisation of a trust broker is essentially an operational matter and, as "broker" suggests, does not affect the overall trust relationship (and associated obligations) between the relying party and the credential issuer.

6. Authentication Model Assessment

6.1 Comparison of Authentication Models

There are a number of perspectives from which to assess the strengths and weaknesses of the above models and their applicability to the various requirements of agencies.

Table 1 highlights key differentiating characteristics between the implementation models. It is intended to inform rather than be authoritative in relation to the nature and implications of these characteristics.

Note: In the table, the characteristics detailed for ‘Federated Portal’ are applicable to the ‘Peer to Peer Portal’ and ‘Federated Portal PLUS’ models.

This document is currently under review by the Digital Transformation Office.

Table 1: Differentiating Characteristics of e-Authentication Models

Attribute	e-Authentication Implementation Models			
	Siloed	**Centralised**	**Federated Portal**	**[2]Federated Authentication Services**
Identifiers and their usage	Identifiers are issued on an application or agency basis and are typically specific to usage within a particular application system.	Identifiers are issued to subscribers which can be leveraged across all agencies that utilise the centralised authentication model.	Identifiers issued by the credential issuer are masked from agencies by the authentication portal which provides agencies with an agency-specific pseudonymised identifier in its place.	Identifiers issued by the credential issuer are not used by, or maintained within agency systems or within authentication services providers.
User centricity in respect to credentials	Typically a single credential will be issued to subscribers for use across all applications within the agency. The issued credential will not be usable outside this domain.	Typically a single credential will be issued to subscribers for use across all applications within participating agencies. The issued credential will not be usable outside this domain.	Subscribers may elect to use one or more credentials in their dealings across government agencies, and revoke credentials and re-enrol with agencies at any stage, subject to agency restrictions.	Subscribers may elect to use one or more credentials in their dealings across government agencies, and revoke credentials and re-enrol with agencies at any stage, subject to agency restrictions.
Privacy considerations and implications	Identifiers are agency specific and as such linkage of information outside the agency through the identifier is not possible.	The use of a single identifier for use across agencies supports the linkage of subscriber information held by participating agencies under suitable authority.	The portal maintains an index of pseudonymised identifiers used in subscriber's dealings with various agencies. As such, a subscriber's dealing across agencies could be determined under suitable authority.	The authentication service maintains a record of usage of a credential by particular agencies but has no means to link this usage to a particular subscriber.

[2] The characteristics detailed for 'Federated Portal' are applicable to the 'Peer to Peer Portal' and 'Federated Portal PLUS' models.

Attribute	e-Authentication Implementation Models			
	Siloed	**Centralised**	**Federated Portal**	**[2]Federated Authentication Services**
Visibility by agencies of the authentication method or processes	Agency systems require visibility of the credential type and related authentication protocols. The credential type might include certificate, OATH OTP etc which have standardised methods of authentication. Transition to new authentication credentials requires modification to agency systems.	Agency systems require visibility of the credential type and related authentication protocols. The credential type might include certificate, OATH OTP etc which have standardised methods of authentication. Transition to new authentication credentials requires modification to agency systems.	Agencies have no visibility or interest in the nature of the subscriber's credential, beyond its assurance level and validity status. This supports simple transition to new authentication methods as they become available or required, without impact on the relying application.	Agency systems typically require visibility of the credential type and related authentication protocols. The credential type might include certificate, OATH OTP etc which have standardised methods of authentication. Transition to new authentication credentials requires modification to relying party systems. The use of authentication service brokers reduces this constraint.
Registration Assurance Levels	Determined and implemented by the agency through reference to NeAF.	Registration Assurance levels are implicit within the subscriber's authentication credential, with the binding to the registered subscriber and the issued credential being created at the time of enrolment.	Registration of subscribers is completed by agencies to an assurance level determined by the agency through reference to NeAF. The effective registration assurance level that is ultimately (late) bound to the issued credential is a function of both the strength of the original registration process and the strength of the enrolment process as discussed above. The effective assurance level is agency specific and applies only to the credential's usage within the agency.	Registration of subscribers is completed by agencies to an assurance level determined by the agency through reference to NeAF. The effective registration assurance level that is ultimately (late) bound to the issued credential is a function of both the strength of the original registration process and the strength of the enrolment process as discussed above. The effective assurance level is agency specific and applies only to the credential's usage within the agency.

Attribute	e-Authentication Implementation Models			
	Siloed	**Centralised**	**Federated Portal**	**[2]Federated Authentication Services**
Agency onboarding processes for subscribers	Agencies electing to implement siloed identity authentication models must implement all elements of the model including registration, credential issuance and management and credential verification services, Moreover, for high assurance needs, agencies must issue security devices to their subscriber base.	Agencies must: • Develop interfaces to the credential issuers credential verification and validation service. • Potentially manage changes (reissuance, replacement etc) in subscriber credentials.	Agencies must develop interfaces to the authentication portal to process: • Authentication assertions received from the service, and • Enrolment requests from subscribers with associated subscriber – credential binding support.	Agencies must develop interfaces to the authentication service to: • Initiate authentication requests to the service and process a range of request responses • Process enrolment requests from subscribers with associated subscriber – credential binding support; and • Manage changes (reissuance, replacement etc) in subscriber credentials.
Potential extensibility to a fully federated identity management environment	Not applicable.	Requisite changes are largely under the control of the centralised authentication service provider. As the provider is already capturing identifying information in support of the service, extensibility of a centralised service to a federated environment is potentially feasible.	The New Zealand government has recently extended its single sign-on product GLS to incorporate an Identity Verification Service as described briefly above. Implementation of similar services as extensions to an authentication portal such as AGOSP through extension of the currently basic user account is considered feasible. Implementation of such a facility would clearly require careful consideration from a privacy perspective.	Extension to a fully federated identity management environment is inconsistent with this model (both technically and philosophically) which is founded on full separation of subscriber identity from the authentication service.

Attribute	e-Authentication Implementation Models			
	Siloed	**Centralised**	**Federated Portal**	**[2]Federated Authentication Services**
Extensibility in respect to technology / discipline and standards advances	Dependent upon the technology and standards deployed within the siloed solution.	Dependent upon the technology and standards deployed within the centralised solution.	It is likely that authentication portal development will be based around existing and emergent standards in this area and in particular SAML, an XML based framework for creating and exchanging authentication and attribute information between entities over the Internet.	It is likely that authentication services development will be based around existing and emergent standards in this area and in particular SAML, an XML based framework for creating and exchanging authentication and attribute information between entities over the Internet.
Extensibility to support authentication of complementary attributes including document and transaction authentication	Dependent upon the technology and standards deployed within the siloed solution.	Dependent upon the technology and standards deployed within the centralised solution.	In itself a federated portal does not provide the infrastructure to support these extended authentication needs. Extension to the model to incorporate future authentication needs is considered feasible.	As the relying party has direct communication with the authentication service it is well placed to implement extended functions such as transaction signing, provided these services are supported by the authentication service.
Supportability of other government and private sector issued credentials	It is unlikely that a siloed implementation would have the necessary infrastructure components to support external credentials without significant extension.	Relying agency systems would need to be modified to interface with other credential issuers and verifiers.	The introduction of third party credentials is fundamental to federated identity management. Nonetheless early and careful consideration would be required on the nature of any future issuers and in particular on how they would be integrated with agency systems either directly or via an existing service provider.	The introduction of additional credential issuers would potentially require awareness of these issuers to be implemented within agency applications. The availability of service brokers, as recently contemplated within Vanguard would serve to partially abstract relying applications from these changes.

This document is currently under review by the Digital Transformation Office.

Attribute	e-Authentication Implementation Models			
	Siloed	**Centralised**	**Federated Portal**	**[2]Federated Authentication Services**
Model maturity and deployed base, including international experience	Siloed implementations have been in place for many years. Most implementations are based on obsolete technology and standards.	Centralised models are in widespread use globally and are well suited to many environments.	Federated models in a variety of incarnations are gaining increased favour globally. Many of the technologies which underpin federated approaches are now also widely used in authentication services, centralised and siloed environments. Standards such as SAML are maturing and full interoperability across suppliers is likely.	The technologies involved in implementation are well proven and can be adapted to support a range of authentication mechanisms and interfaces including assertion based protocols such as SAML and legacy interfaces such as Radius.
Legal, contractual and governance requirements and implications	Not applicable.	Centralised services typically operate under scheme rules and regulations that define key operational characteristics as described previously. Centralised services are likely to have fewer operational participants than federated models and consequently fewer arrangements to be considered.	A range of arrangements can be implemented to support operations within a federated environment. These include scheme based arrangements, multilateral arrangements and bilateral arrangements.	It is most likely that arrangements would exist between each relying party and one or more distinct credential issuers, rather than a broad scheme based arrangement.

6.2 Mapping Service Delivery Models to e-Authentication Models

In practice, selection by agencies or collectives of agencies of the most appropriate authentication model for their business applications and service delivery models will be determined by a range of issues and influences including those presented in Table 1.

Notwithstanding the above, Table 2 below provides an indicative mapping of the suitability of various identity authentication implementation models described in section 3.3 to the service delivery models described in section 2.1.

Table 2: Rating suitability of e-Authentication Models to Service Delivery Models

e-Authentication Models	**Service Delivery Models**		
	Sectoral	**Agency Cluster**	**WoG**
Siloed			
Centralised	✓✓✓(1)	✓(1)	
Federated- (SSO) Portal	✓✓(2)	✓✓(2)	✓✓(2)
Federated Peer to Peer Portal		✓✓(4)	✓✓✓(3)
Federated Portal PLUS		✓✓✓(5)	✓✓✓(5)
Federated Authentication Services			✓✓✓(6)

In Table 2 the number of ticks represents a relative measure of suitability, whilst the number in brackets refers to the explanatory note below.

Explanatory Note

1. Benefits through a single identifier used across the participating agencies.
2. Benefits through a single point of access with a credential.
3. Benefits through increased openness and user choice in use of particular credentials.
4. Benefits through increased openness and user choice in use of particular credentials. Agency overheads through increased operational complexity.
5. Potential benefits through user authorised synchronisation of identity related information across participating agencies.
6. Benefits through implicit separation of users' affairs across agencies without the loss of user benefit of single credential usage.