Australian Banking Association

Guiding Principles for Accessible Authentication

Acknowledgements

The Guiding Principles for Accessible Authentication ("The Guiding Principles") were funded and developed under the sponsorship of the Australian Banking' Association (ABA). The ABA would like to acknowledge the contribution of the Human Rights and Equal Opportunity Commission (HREOC), Blind Citizens Australia, Physical Disability Council, Abacus Australian Mutuals and various ABA member banks that participated in the ABA's Accessible Authentication Working Group (AAWG).

The ABA would also like to acknowledge Tim Noonan for his work on this project and Dr John Gill for allowing us to use the *Guidelines for the Design of Accessible Information and Communication Technology Systems*, in particular the section on biometric systems.

The ABA released the Consultation Draft Guiding Principles on Accessible Authentication to coincide with International Day of People with a Disability on 3 December 2006, with the theme being accessibility to information technologies "E-Accessibility Day". The ABA would also like to acknowledge the Council of the Ageing (COTA) and other organisations representing people with disabilities or older people for providing valuable input into the development of the Guiding Principles.

Disclaimer

The ABA and all other parties associated with the publication of this document, have made every effort to ensure the accuracy of information, but accept no responsibility for any loss or damage occasioned by any party in its seeking to implement any provision of the Guiding Principles.

The Guiding Principles are based on information about the deployment of authentication technologies available at the time they were developed.

The Guiding Principles should not be relied upon as a substitute for professional advice in complying with the law. There are many liability and other legal issues relating to matters covered in the Guiding Principles, the resolution of which falls outside the scope of the document. Future versions of the document will endeavour to incorporate the latest research.

The Guiding Principles have been developed by the AAWG and drawn from a number of other sources, it must only be reproduced with permission from the ABA and attribution to the ABA. If material is referred to by other people or organisations, attribution must be made to the ABA.

Published by the Australian Banking Association Inc
ARBN 117 262 978
Incorporated in New South Wales
Liability of members is limited
Version: December 2007

Table of Contents

“The Guiding Principles”

Principle 1: Accessibility of authentication technologies
Financial institutions should ensure that authentication technologies are accessible to all customers, or where this is not possible, a human-based alternative authentication system needs to provide equivalent amenity and convenience.

Principle 2: Customer convenience
All customers should be able to undertake their personal and business financial activities conveniently and safely.

Principle 3: Authentication planning
Financial institutions should consider the accessibility needs of customers with disabilities and older customers as part of authentication technology planning.

Principle 4: Authentication testing
Financial institutions should consult customers with disabilities and older customers as part of planning and testing accessibility of authentication technologies.

Principle 5: Registration, login and transaction procedures
Financial institutions should ensure that registration, login and transaction procedures are as accessible as possible to all customers.

Principle 6: Messages and error recovery
Financial institutions should ensure that online messages are unambiguous and written in “plain English” and that error recovery processes are efficient and accessible.

Principle 7: Staff and customer training
Financial institutions should provide relevant customer support staff with appropriate disability awareness training so they are aware of the needs of customers with disabilities and older customers. In addition, financial institutions should provide customers with information and training in the use of available authentication technologies.

Principle 8: Raising staff, business and customer awareness
Financial institutions should develop a strategy for enabling relevant management and staff awareness of these Guiding Principles. In addition, financial institutions should promote the availability of alternative accessible authentication technologies with their customers.

Principle 9: Confidentiality of customer information
Financial institutions must ensure the confidentiality of information of customers with disabilities and older customers.

Principle 10: Security of transactions and transaction fees
Financial institutions should ensure customers with disabilities and older customers are not exposed to higher financial risks or costs as a result of the deployment of authentication technologies.

1. Introduction

1.1 Background to the Guiding Principles

All organisations providing goods, services and facilities to the general public must ensure they are not provided in a way that is discriminatory.

Conducting banking and managing personal finances are important activities. Advances in technology and the emergence of electronic banking have increased the convenience of banking, but have also increased the need for financial institutions to make sure that their customers can conduct their banking safely and securely.

Accessibility issues need to be considered in the deployment of authentication technologies, to ensure that people with disabilities and older people are not disadvantaged. Adoption of common standards by banks and other financial institutions in Australia will promote the confidence of customers using authentication technologies and improve the accessibility of retail banking and finance.

The Guiding Principles have been developed to:

- Provide guidance to financial institutions adopting stronger authentication[1] technologies as part of their banking services;
- Ensure that all customers of financial institutions operating in Australia, including people with disabilities and older people, are able to access and manage their finances independently, securely and effectively;
- Ensure that the access needs of people with disabilities and older people are considered in the deployment of authentication technologies; and
- Ensure that financial institutions are able to provide the best possible service to all customers.

1.1.1 Disability Discrimination Act 1992

The *Disability Discrimination Act 1992* ("DDA") makes it unlawful to discriminate against a person on the grounds of a disability[2]. The objects of the DDA include eliminating, as far as possible, discrimination against people with disabilities and promoting recognition and acceptance within the community that people with disabilities have the same fundamental rights as the rest of the community.

[1] 'Stronger authentication' refers to any authentication strategies considered stronger than conventional single-factor authentication, such as two-factor, multi-factor, strengthened single factor and anti-keylogging strategies. For more information, see page 26.

[2] Section 4 of the DDA defines disability in relation to a person as:
(a) total or partial loss of the person's bodily or mental functions; or
(b) total or partial loss of a part of the body; or
(c) the presence in the body of organisms causing disease or illness; or
(d) the presence in the body of organisms capable of causing disease or illness; or
(e) the malfunction, malformation or disfigurement of a part of the person's body; or
(f) a disorder or malfunction that results in the person learning differently from a person without the disorder or malfunction; or
(g) a disorder, illness or disease that affects a person's thought processes, perception of reality, emotions or judgment or that results in disturbed behaviour;
(h) and includes a disability that:
(i) presently exists; or
(j) previously existed but no longer exists; or
(k) may exist in the future; or
(l) is imputed to a person.

The law is administered by HREOC and sets out specific areas in which it is unlawful to discriminate. These areas include accommodation, employment, access to premises, and the provision of goods, services[3] and facilities.

The DDA recognises that in certain circumstances, providing equitable access for people with disabilities could cause 'unjustifiable hardship' for an individual or organisation providing goods or services.

1.1.2 Human Rights and Equal Opportunity Commission

The Human Rights and Equal Opportunity Commission (HREOC) administers Federal legislation in the area of human rights, anti-discrimination and social justice. This includes complaints handling, public inquiries, policy development and education and training.

Where a person with a disability believes they have been discriminated against, they can complain to HREOC who will investigate the complaint and, where appropriate, attempt to conciliate a solution between the two parties. Where conciliation is not possible the complainant may take their complaint to the Federal Court or Federal Magistrates Court who have the authority to determine whether unlawful discrimination has occurred and what constitutes 'unjustifiable hardship'.

HREOC also has a role in assisting organisations understand their responsibilities and supporting initiatives aimed at promoting compliance through best practice. While the Guiding Principles have no force in law, HREOC has supported their development in the hope that they will provide a level of access consistent with the requirements of the DDA.

1.2 Purpose of the Guiding Principles

The purpose of the Guiding Principles is to provide a framework for financial institutions to help reach a workable balance between security requirements, commercial strategies and equitable access to banking products and services.

The Guiding Principles are intended to promote the following universal design principles: [See http://www.design.ncsu.edu/cud/about_ud/about_ud.htm]

- **Equitable use**: The design is useful for the widest possible group of users.
- **Flexible use**: The design accommodates a wide range of individual preferences and abilities.
- **Simple and Intuitive use**: The design is easy to understand.
- **Perceptible use**: The design communicates necessary information to the user in a clear and effective manner.
- **Tolerance for error**: The design minimises hazards and the adverse consequences of accidental or unintentional actions.
- **Minimal physical effort**: The design can be used comfortably.
- **Size and space for approach and use**: The design can be used conveniently.

[3] Section 4 of the DDA defines a service as relating to, amongst other things, banking, insurance, superannuation and the provision of grants, loans, credit or finance, and including financial and information services provided, for example, through websites, telephones, ATMs and EFTPOS.

The Guiding Principles have been developed to ensure that people with disabilities and older people are not discriminated against when a financial institution adopts stronger authentication technologies and systems. They seek to make sure that authentication technologies are as accessible as possible for as many customers as possible.

The Guiding Principles offer a number of benefits for financial institutions, including enabling financial institutions to manage risk, improve quality of services and reduce the likelihood of successful complaints of discrimination arising from access to banking products and services.

The Guiding Principles recognise that:

- Financial institutions need to ensure that fraud is minimised and need to manage customer confidence and the financial institution's financial risk.
- People with disabilities and older people need to be able to access their finances and conduct business efficiently, conveniently, independently and on an equivalent basis as other customers.
- Financial institutions need the flexibility to develop security and authentication systems which effectively integrate into their business rules, are consistent with their commercial strategies, and which they deem appropriate to meet the needs of their customers.

1.3 Scope of the Guiding Principles

The Guiding Principles relate to deployment of user and transaction authentication technologies and systems across retail banking channels, with particular relevance for electronic banking.

The Guiding Principles focus on access to authentication technologies for individual and small business customers registering, using and transacting with their financial institution. They do not relate to wider technology matters than those related to deployment and use of authentication technologies. However, financial institutions may consider how the Guiding Principles could relate to wider usability and their broader service commitments on accessible banking.

Examples of transactions covered by the Guiding Principles include, but are not limited to:

- Service registration
- Balance enquiry
- Statement viewing
- Transfers between accounts
- Bill pay
- Third party funds transfers
- Cash withdrawals
- Reviewing and updating investments and portfolios
- Online loan applications
- Interactive financial calculations performed online.

The Guiding Principles also apply to related services such as accessing documentation and information as well as account aggregation tools where authentication technologies are deployed.

The Guiding Principles are intended for use by developers, suppliers, designers and users of authentication technologies. They are not intended to prevent the use of authentication technologies.

The intended audience for the Guiding Principles includes banks and other financial institutions as well as other stakeholders including regulators, government agencies and law enforcement bodies. They are also relevant to disability organisations, individuals with disabilities and older people.

1.3.1 Dependencies

A range of factors can impact the effective accessibility of retail banking services including:

(a) (for the financial institution) choice of authentication solutions, web development tools, expectation of minimum hardware/browser technology used by customer, reliance on scripting and applet technologies, flexibility of security protocols in place.

(b) (for the customer) level of experience with web-based technologies, platforms/operating systems selected, brand and version of assistive technologies (screen readers, screen enlargers, etc), firewalls and quality of telecommunications lines and other factors.

1.4 Principles-based approach of the Guiding Principles

The Guiding Principles are high level principles that do not prescribe binding obligations and do not provide technical standards. It is up to financial institutions to determine how to apply the Guiding Principles.

In implementing the Guiding Principles, financial institutions will set their own boundary conditions on threat levels, transaction values and other parameters, being mindful of the accessibility implications of any authentication technologies deployed.

The Guiding Principles recognise that financial institutions should make best endeavours to ensure that authentication technologies are as accessible as possible for as many customers as possible.

1.4.1 Compliance with other access standards

Banks and other financial institutions should also refer to relevant Australian standards, Australian/New Zealand standards and other international standards. For example:

- ABA's voluntary *Industry Standards on Accessibility of Electronic Banking*
- ABA's voluntary *Online Authentication Guidelines*
- HREOC's World Wide Web Access: Disability Discrimination Act Advisory Notes. Version 3.2.
- W3C's Web Content Accessibility Guidelines.

1.5 Technology Neutrality of the Guiding Principles

The Guiding Principles set out broad concepts that may be applied across the range of retail banking channels. This approach was taken so that the Guiding Principles could be applied to a variety of authentication technologies and solutions, including those which do not yet exist.

The Guiding Principles are intended to be technology neutral. They do not recommend specific authentication technologies. Instead, the Guiding Principles set out high level principles and provide explanatory guidance on how these principles may assist develop technical and design specifications and performance criteria that can be used to assess the appropriateness and usability of authentication technologies and systems in the context of each individual financial institution's circumstances. Decisions regarding specific authentication technologies are, amongst other things, commercial decisions.

The Guiding Principles also take into account developments that may occur in communications and access technologies, which may be used to interact with authentication technologies, for example, voice over IP (VOIP), video relay services, computer assisted translators and other assistive technologies.

1.6 Adoption of the Guiding Principles

Adoption of the Guiding Principles is voluntary, but it is expected that ABA member banks and other financial institutions, including credit unions and building societies, will seek to take advantage of the benefits afforded by the Guiding Principles.

The Guiding Principles are aimed at assisting financial institutions to design and develop the most accessible authentication systems as possible. They assist financial institutions to respond to the needs of customers and requirements of the *Disability Discrimination Act 1992*. It is intended that adoption and implementation of the Guiding Principles will significantly reduce the likelihood of successful complaints of discrimination.

It is recognised that financial institutions adopting the Guiding Principles may take some time to have in place systems and procedures that reflect the detail of the Guiding Principles and explanatory guidance.

Financial institutions should also consider the ABA's voluntary Industry Standards on Accessibility of Electronic Banking (2002), which assist individual banks develop or enhance their electronic banking services for people with disabilities and older people as well as the ABA's voluntary Online Authentication Guidelines (2005), which provide a risk-based model for the deployment of authentication technologies. The ABA's voluntary industry standards are consistent with, and build on, the W3C's Web Content Accessibility Guidelines.

Financial institutions could also consider referring to the ABA's voluntary Guiding Principles for Accessible Authentication and the voluntary Industry Standards on Accessibility of Electronic Banking in their Disability Action Plans or service commitments, which set out how financial institutions will meet their customers' needs, including equivalent access for people with disabilities and older people.

1.7 Version control and review of the Guiding Principles

It is the intention of the banking and finance sector to continue to work with service providers and manufacturers of authentication technologies to further improve the accessibility of authentication technologies and solutions.

The ABA will continue to keep the Guiding Principles current and technically valid in so far as is practicable. Version control will be maintained by the ABA.

The Guiding Principles will be reviewed on an as needed basis to ensure that they remain current with technology developments and emerging considerations with authentication technologies. However, given that this is the first edition of the Guiding Principles and authentication technologies are a rapidly evolving area, the ABA will conduct an initial review after 12 months.

2. The Guiding Principles

Financial institutions should be mindful of the principles of accessibility and inclusiveness in adopting authentication technologies from concept through to deployment. The aim is to create policies and systems to accommodate the widest possible range of users and customers.

The Guiding Principles cover deployment of authentication technologies, including design, implementation, communication and operation.

Principle 1: Accessibility of authentication technologies

Financial institutions should ensure that authentication technologies are accessible to all customers, or where this is not possible, a human-based alternative authentication system needs to provide equivalent amenity and convenience.

Financial institutions should make best endeavours to ensure that all authentication technologies across retail banking channels are as accessible as possible to all customers.

Authentication technologies should support the widest possible range of customers, including customers with disabilities and older customers, without the need to develop alternative options or 'fall-back' modes of access. However, where this is not possible, alternative authentication should be provided which enables equivalent amenity and convenience. For example, a customer with damaged fingers or motor impairments may have difficulty using biometric authentication technology, which relies on matching a fingerprint to a person. An alternative method of authentication should be available for such customers and may be technology or human-based.

Explanatory guidance to Principle 1

While the expectation is that financial institutions will do all they can to ensure any authentication technologies provide for the greatest possible access for all customers, there may be occasions where alternative authentication processes or systems need to be provided.

A customer may not be able to use an authentication technology because they either have extreme difficulties in one particular area or have multiple disabilities so that no combination of the accessibility features meets their needs. For example, a customer who is both deaf and blind is unable to hear the information in spoken form and is unable to read the authentication information visually. Such a customer most likely needs to have in place Braille technology capable of accessing the National Relay Service/TTY and will need to communicate with a human agent via this service. [See www.relayservice.com.au]

A customer may have motor skill difficulties which make inputting data difficult in the prescribed time period. Such a customer may be better served by a human agent. Alternatively, a customer may be physically able to use the authentication technology, but is encountering confusion or difficulties understanding how to use the authentication due to an information or intellectual disability or age-related cognitive impairment. Such a customer may also be better served by a human agent who is better placed to interpret and suggest remedies for the customer. A human agent also provides a friendly 'face' to the financial institution, particularly when new authentication technologies are being deployed.

If a customer is unable to use a retail banking channel due to the authentication technology deployed, there should be a means by which the customer can gain ‘equivalent access’, such as equivalent funds transfer limits. This may be via automated telephone banking or it may be necessary for the customer to speak to a human agent to enable them to transfer the required amount. Financial institutions should ensure that the process by which a customer is authorised to work with a human agent is straightforward and convenient, such as if forms need to be completed, these forms need to be available in accessible formats.

Financial institutions should consider making available a human agent 24 hours a day, 7 days a week, or at least for extended business hours. A human agent or customer service representative is usually the most effective and convenient solution for those customers that have difficulty in completing their banking transactions due to the authentication technology deployed. Financial institutions should also provide their staff and customers with information explaining authentication technologies, alternative authentication arrangements and banking channels.

Financial institutions should have a dialogue with their customers to identify and put in place suitable access arrangements. Financial institutions may need to develop individual arrangements for some customers that are unable to access banking services due to the authentication technology deployed. For example, some customers may have to make use of human-based alternatives, such as telephone banking, and may need to access services that would otherwise not be available through ordinary telephone banking channels, such as immediate access to make larger payments or transfers and retrieve account statements. In these instances, individual arrangements for such customers unable to conduct their banking transactions due to difficulties using authentication technologies may need to be reflected in business rules and with support services.

Financial institutions should consider how authentication technologies or alternative authentication arrangements deployed to access retail banking channels may impact on the privacy and security of their customers. For example, financial institutions may need to consider how authentication technologies may impact customers using face-to-face banking via bank branches, such as customers who are hearing impaired and utilising counter hearing systems, including microphone and hearing loop at branch counter or an Auslan interpreter. Similarly, financial institutions may need to consider how authentication technologies for telephone banking may impact on customers using support services and authorised third parties to complete their banking transactions, such as the National Relay Service/TTY.

Financial institutions should consider providing a choice of authentication technologies to maximise the number of people who can independently use the authentication technology, access their banking services and conduct their banking transactions. Some authentication technologies rely on the customer being able to see a display, whereas, others may offer possibilities for information to be spoken. Biometric authentication solutions may rely on the person possessing a particular attribute or capability, and therefore will exclude people who are unable to meet the necessary physical requirements. Providing more than one authentication system, such as a variety of tokens (large screen and/or audio), SMS messages, shared secrets and so on, gives choice and broadens the likelihood that a customer can use one of the available authentication approaches.

Financial institutions should provide efficient re-enrollment. If a customer can no longer use an authentication or biometric system reliably, the customer should be provided, wherever feasible, with the opportunity to repeat the registration or enrollment process. For example, this could happen if the customer has an accident, or if their biological attributes change for some reason.

Financial institutions need to consider their business rules to ensure that Powers of Attorney and designated authority representatives (such as a family member, friend, carer or other authorised third party) are appropriately recognised as part of the deployment of authentication technologies. For example, some customers may have third parties assist them in conducting their banking transactions. Formal arrangements should be accommodated within authentication procedures and systems. Financial institutions should also ensure that business rules enable intermediaries and third parties to be authorised on a permanent basis or session/transaction specific basis.

Financial institutions should be aware that some of their customers use support services and/or assistive technologies to help them verify their identity, access their banking services, conduct their banking transactions and verify their transactions, which may mean these customers may take longer than other customers to complete their banking activities. Financial institutions should ensure their staff and customers are aware that customers using support services and/or assistive technologies may take longer to complete their banking activities.

Financial institutions should ensure their customers have access to the support services of qualified and reputable interpreters to assist them conduct their banking transactions, such as interpreters accredited to the National Accreditation Authority for Translators and Interpreters (NAATI). For example, financial institutions should make available information about how to access qualified and reputable support services.

Financial institutions should consider 'equivalent access' not just in design and deployment of authentication technologies, but as part of staff and customer training and awareness.

Principle 2: Customer convenience

All customers should be able to undertake their personal and business financial activities conveniently and safely.

Authentication technologies should be designed and deployed so that the widest possible range of customers can use the technology effectively and conveniently. Authentication solutions should be as user-friendly and accessible as possible.

Financial institutions should provide information to customers on user requirements for authentication technologies, and alternative authentication technologies available for those customers unable to meet the user requirements.

Financial institutions should ensure that all customers can access their banking services conveniently. Some factors to consider include support services, such as the National Relay Service/TTY or Auslan interpreters, other authorised third parties acting on behalf of customers and other mechanisms that help customers conduct their banking activities.

Financial institutions could work with relevant community organisations to identify strategies that promote customer convenience as well as minimise the possibility of financial abuse by ensuring arrangements and processes are in place to support alternative authentication options, such as business rules, Powers of Attorney and other formal authorisations.

Explanatory guidance on Principle 2

All customers benefit from universal designs, however, it is important to understand the diversity of problems, tools and abilities of all customers, especially those customers with disabilities or older customers who may find it particularly difficult to access banking services where authentication technologies are deployed.

Financial institutions should also ensure they comply with the W3C's Web Content Accessibility Guidelines. As consistent with W3C/WAI, to promote user convenience:

- Content must be perceivable: For example, provide text alternatives for all non-text content and make it easy to distinguish foreground information from its background.

- Interface components in the content need to be operable: For example, make all functionality operable via a keyboard interface; allow users to control time limits on their reading or interaction or allow users to extend a session that is about to time out; and help users avoid mistakes and make it easy to correct mistakes that do occur.

- Content and controls must be understandable: For example, make text content readable and in "plain English".

- Content should be robust enough to work with current and future users, including assistive technologies: For example, ensure that content is accessible or provide an accessible alternative.

Financial institutions should make every effort to support the widest possible range of customers. Beginning with their own organisations, financial institutions should work towards consistency of Internet-related terminology, concepts and processes, with the following objectives:

(a) consistency of standard transactions across financial institutions, for example, by agreeing on order of fields in funds transfer forms, BPAY forms, etc;

(a) consistency on terminology for user name, password, receipt number, etc. (Experience has shown that consistent and predictable human interfaces benefit users. The benefits can include faster learning, greater productivity, fewer errors and greater satisfaction. Consistent interfaces also benefit the industry by promoting greater acceptance of products and services.)

The following notes from W3C/WAI should also be considered:

> "Provide consistent and predictable responses to user actions within the online service. Make interactions consistent, both throughout the site and with commonly used interaction metaphors used throughout the Web. For example, similar layout for user interface components is used throughout your site, similar user interface components are labelled with similar terminology, controls that look the same are designed to act the same, operating system, language, or application conventions likely to be familiar to the user have been followed, unusual user interface features or behaviors that are likely to confuse the first-time user are documented. Providing responses to user actions is important feedback for the user. This lets them know that your site is working properly and encourages them to keep interacting. When the user receives an unexpected response, they might think something is wrong or broken. Some people might get so confused they will not be able to use your site."

Principle 3: Authentication planning

Financial institutions should consider the accessibility needs of customers with disabilities and older customers as part of authentication technology planning.

Financial institutions should consider the access requirements of customers with disabilities and older customers in the design of authentication technologies. It is good business sense to ensure all customer needs are considered early in the design and implementation of authentication technologies in order to avoid incurring potential additional costs later.

<u>Explanatory guidance on Principle 3</u>

Financial institutions should consider the accessibility needs of customers with disabilities and older customers in the design of authentication technologies. When planning to implement authentication technologies, financial institutions should consider how the authentication technologies they deploy may impact all customers. By taking into account the needs of all customers and the environments in which they work, authentication technologies can both enhance security and provide convenient access. For example, accessibility considerations could be part of any internal check-lists used by financial institutions when assessing, developing or modifying authentication technologies.

Financial institutions should consider the accessibility implications and processes for stronger authentication. There are three phases involved in stronger authentication approaches.

- Enrolment – Setting up the technology, registering the customer, taking necessary details or measurements, issuing devices/passwords etc. If a biometric system is used, enrolment involves taking a baseline biometric measure. Usually, this would be done with a special biometric terminal, which should be staffed by qualified personnel. Those personnel should be trained in the necessary skills to assist a person with a disability to successfully provide the biometric measure or measures.

- Authentication – Identity of the person is validated and verified to a satisfactory degree, based on the information and credentials being supplied by the user.

- Authorisation – Once the authentication has been done, the customer is then allowed access to those services and information which they are authorised to access.

Some key points to consider when ensuring maximum flexibility for financial institutions and users include:

- Authentication management – roles and responsibilities will most likely spread across business units; for example, authentication policies and procedures, user enrolment, applications and networks and so on. It is important that deployment of user authentication technologies is effectively managed.

- Authentication practices – existing practices and user privileges should be accommodated. Balancing security, usability and practicality will assist in adoption of new technologies. It is important for financial institutions to maintain flexibility to support multiple users without incurring undue cost.

- Authentication integration – a review of users, applications and environments when introducing new system requirements should be conducted. It is important to reduce unnecessary or costly system integrations later.

- Technology neutrality – as far as possible, authentication architecture should be interoperable with different applications and/or devices. It is important for users to maintain autonomy in selecting technology or applications to access Internet banking services.

Financial institutions should ensure that authentication technologies do not impede their ability to meet standards on accessibility of electronic banking. For example, consideration of timed responses should be included in authentication planning.

Financial institutions should consult existing standards for accessibility, such as the ABA's voluntary Industry Standards on Accessibility of Electronic Banking and the W3C's Web Content Accessibility Guidelines.

Principle 4: Authentication testing

Financial institutions should consult customers with disabilities and older customers as part of planning and testing accessibility of authentication technologies.

Financial institutions should test accessibility of their authentication technologies and solutions through user accessibility trials.

Financial institutions could consult with organisations representing people with disabilities or older people to identify a representative panel of end-users.

Financial institutions may also consult with accessibility experts to ensure wide testing of possible authentication technologies and solutions.

Explanatory guidance on Principle 4

During design, and prior to implementation, financial institutions should test accessibility of their authentication technologies, including all elements of the interface, with users representing a range of capabilities and limitations (such as, in respect of visual, auditory, physical, cognitive and behavioural ability). For example, to test accessibility of their authentication technologies and solutions, financial institutions could conduct user accessibility trials. Such trials could be engaged to identify potential authentication issues and should involve a representative panel of end-users covering a range of users, including users with disabilities and older users.

Organisations that may assist in identifying potential end-users to be engaged in testing can be found at the HREOC website. [See 'Peak/major organisations' at www.humanrights.gov.au/disability_rights/links/links.html#community]

There are significant benefits to consulting with customers and users from the beginning of the project (for example through focus groups at the initial planning stages) and at key stages within the project. Feedback from customers and users can then be incorporated into the business rules and user requirements that create a framework for the development of technical and design specifications and performance criteria. This may help minimise accessibility problems after implementation.

Financial institutions should test their authentication technologies with adaptive and assistive technologies, such as screen readers, screen enlargers, speech recognition software and computer assisted translators. Testing should also be conducted using various web browsers to ensure wide accessibility.

There are also significant benefits in testing accessibility for wider usability. Decisions concerning accessibility are unlikely to adversely affect overall usability, and in fact, these decisions can often enhance usability for all customers. However, if changes are made for accessibility, the revised design may need to be tested again for general acceptance.

A range of semi-automated evaluation and testing tools is available on the W3C website. [See http://www.w3.org/WAI/ER/tools/]

Principle 5: Registration, login and transaction procedures

Financial institutions should ensure that registration, login and transaction procedures are as accessible as possible to all customers.

Implementation of stronger authentication should, as far as possible, not substantially compromise convenience of registration, login and transaction procedures.

Financial institutions should provide an opportunity for customers to identify that they may require alternative authentication.

Authentication procedures required for registration, login and transactions should, as far as possible, be able to be operated by customers who use access and assistive technologies, such as alternative input software and screen output software to assist accessing technology, including speech recognition or screen reading software for Internet banking.

Explanatory guidance on Principle 5

Authentication technologies and systems should provide timeouts of sufficient duration so that all customers have adequate time to look up and enter their password. For example, financial institutions should consider authentication technologies that enable flexibility to alter or extend the time required to complete authentication. Alterations to authentication should not undermine security requirements.

Financial institutions should follow the guidance recommendations on account and service registration found in section 11.4.1 and on timeouts found in section 11.1.2.1 of the ABA's voluntary Industry Standard on Internet Banking.

Financial institutions should, subject to identification and security requirements, accept the registration of a customer to an Internet banking service when the registration request is received either directly via a telephone or TTY, or indirectly through a telephone relay service, and without completing printed forms. Customers should, as far as possible, be able to use a keyboard alternative. For this to occur, an arrangement may need to be put in place with the financial institution to recognise the disclosure of confidential information between those parties to the arrangement as an individual arrangement and as an exception to standard business rules.

Principle 6: Messages and error recovery

Financial institutions should ensure that online messages are unambiguous and written in "plain English" and that error recovery processes are efficient and accessible.

Financial institutions should make best endeavours to ensure that all customers are able to easily and readily understand error messages and undertake error recovery processes. For example, customers should, as far as possible, be provided with the opportunity to recover or cancel transactions or change data.

Financial institutions should ensure that error messages presented to the customer by authentication technologies are clear and unambiguous. For example, some customers, particularly those with intellectual disabilities or cognitive impairments, may find it difficult to comprehend some automated error messages. Error messages generated by financial institutions should be relevant to the error, for example, "failed authentication".

Explanatory guidance on Principle 6

Customers should, as far as possible, be provided with the opportunity to recover from their most recent error without being required to re-enter correct information. Customers should also, as far as possible, be provided with the opportunity to cancel transactions and/or change data and information that has been entered during a session without having to cancel the session and re-commence.

Authentication technologies may require some information to be re-entered so that system and account security is not compromised. Errors can occur for a variety of reasons and therefore sometimes re-prompting of previously entered data may be required to reinitiate retail banking services or confirm transactions. Where it is not possible to recover from an error, for example, after submitting and confirming a payment, financial institutions should provide a confirmation for customers to check transaction details before submitting payments and understand that authentication was successful and the transaction and/or payment successful. Confirmation is important for authentication and can also enhance usability for all customers. Confirmation screens or confirmation notifications, such as that an action has occurred, i.e. "successful authentication" or a transaction has taken place, should be accessible.

Within a given session, unless information re-entry is required for reasons of privacy, security or verification, the customer should not be required to enter any given piece of information more than once. For example, the number of key presses or mouse clicks required of the user should be minimised.

Redundancy of information across more than one sensory channel should be provided, and will assist customers with sensory disabilities as well as all customers that use personal/mobile technologies. For example, video clips should contain audio descriptions for blind users and text captions for deaf users.

Audible bells and alarms from the computer should also be represented visually. Pictures, tables, flow charts and other visual information should be described or summarised in textual form, where possible, for those who cannot see them and for those who do not have graphical capabilities readily available.

When live streaming is used, text script should be provided as soon as possible following the event.

Customers should have access to 'Help' functionality to assist in identifying and fixing connectivity problems. Financial institutions should provide online access to assist on common error messages, such as in the form of accessible FAQs. Help desk should also be available to assist customers in completing authentication and accessing their retail banking services.

In instances of system failure, financial institutions should ensure that error messages allow customers to easily and readily recover and clearly state procedures for customers to reinitiate their banking transaction or activity. For example, customers may be required to re-enter information to recover from data or information loss, which may not be apparent to users of authentication technologies.

Financial institutions should follow the guidance recommendations on error recovery found in section 11.4.6 of the ABA's voluntary Industry Standard on Internet Banking.

Principle 7: Staff and customer training

Financial institutions should provide relevant customer support staff with appropriate disability awareness training so they are aware of the needs of customers with disabilities and older customers. In addition, financial institutions should provide customers with information and training in the use of available authentication technologies.

Relevant staff whose primary role is to provide customer support services should be provided with appropriate awareness training to understand that some customers may use access and assistive technologies, such as screen readers, screen enlargers, speech recognition software, computer assisted translators, or authorised third parties, such as the National Relay Service/TTY, to assist them in accessing and conducting their banking activities.

Financial institutions should make available information about how to effectively and securely use authentication technologies.

Financial institutions should consider how best to deliver information and training in the use of authentication technologies specifically designed to meet the needs of customers with disabilities and older customers. For example, financial institutions could provide customer training through a range of methods, such as web-based, DVD/CD-rom, over the telephone or face-to-face. Training should be delineated by media types, such as captioning and audio description.

Explanatory guidance on Principle 7

It is important that training is accessible for people with disabilities and older people. Financial institutions should provide access to appropriate learning opportunities for their staff and customers, as part of eliminating the 'Digital Divide'.

Financial institutions should provide relevant staff with training relevant to their position or role within the organisation. Training should be part of induction and initial training programs and ongoing training programs, especially for staff that are in customer-facing roles.

Managers, supervisors and senior staff in branch, call centre customer service and help desk functions should be provided with appropriate awareness training in the combination of authentication and access technologies and in understanding how people with disabilities and older people access online services. For example, financial institutions could consider making available a staff member with superior knowledge and skills in dealing with customers with a disability or older customers in a branch, call centre customer service or help desk function.

Financial institutions should provide relevant branch, call centre customer service and help desk staff with appropriate training in providing support for users of authentication.

Some topics could include:

- Basic facts about people with disabilities and access to online services;

- Information about tools and equipment that may be used to read information, such as screen readers;

- Information about different formats and how the organisation is using different formats for people with disabilities, such as Braille statements; and

- Identification of appropriate induction and ongoing training areas where face-to-face and e-learning about accessibility of banking can be incorporated.

Staff who are web developers and/or web content managers should receive training and guidance in developing accessible websites and in understanding how people with disabilities and older people access online services, so that they can develop appropriate strategies for authentication and broader accessibility of Internet banking websites.

Staff who are employed to assist customers operate biometric terminals or support systems which employ authentication technologies should be trained in how to assist and support customers with disabilities and older customers.

Customer training will ensure that all customers are able to easily, readily and efficiently access and operate authentication technologies. Training should be developed taking into account all customer needs, including the needs of customers with a range of capabilities and limitations.

Financial institutions should make available training in the use of authentication technologies specifically designed to meet the needs of staff and customers with disabilities and older staff and customers, such as training provided through a range of methods including web-based, DVD/CD-rom, over the telephone or face-to-face.

Where financial institutions provide face-to-face training, this should be developed and conducted by suitably trained staff, or could be offered by arrangement with a registered training organisation (RTO) with experience in training people with disabilities and older people.

Where financial institutions provide customer training over the telephone, training staff should be capable of providing support to people with disabilities and older people. Where financial institutions provide customer training via DVD/CD-rom or web-based formats, training should be delineated by media types.

Some areas to cover in training modules could include:

- Practice Option: Each site should have a practice section, where people can perform practice logon and trial transactions to safely explore and master the service, without risking funds. To ensure accessibility, the practice facility should provide a substantially similar customer experience and should give feedback on the success or otherwise of the practice transaction. Such feedback should also include suggestions on error correction.

- Accessible Online Tutorials: Users may benefit from accessible online tutorials for a site or feature. To ensure accessibility, tutorials should be developed using the same technologies as for the actual service.

Financial institutions should consider providing all staff with training regarding awareness of the needs and diversity of people with disabilities and older people as part of staff induction training and ongoing workplace diversity programs.

Principle 8: Raising staff, business and customer awareness

Financial institutions should develop a strategy for enabling relevant management and staff awareness of these Guiding Principles. In addition, financial institutions should promote the availability of alternative accessible authentication technologies with their customers.

Financial institutions should ensure relevant management and staff have a broad awareness of the diversity of their customer base and accessibility issues, including the existence of these Guiding Principles.

Financial institutions should promote the availability of alternative accessible options to help customers with disabilities and older customers to become aware of authentication technologies and possible alternative authentication arrangements or devices. Promotion of these alternative arrangements or devices could be done in partnership with organisations representing people with disabilities or older people.

Relevant banking information and marketing materials about authentication technologies should contain information on devices and services to support all customers.

Financial institutions should also discuss with relevant organisations and representatives of people with disabilities and older people issues about privacy and security rights and responsibilities of customers of authentication technology and reflect outcomes of discussions in individual organisation's policies and business rules.

Explanatory guidance on Principle 8

It is important for there to be relevant management and staff awareness of the diversity of their customer base and accessibility principles.

Financial institutions should consider how best to advocate and raise awareness of accessibility issues within the organisation. For example, financial institutions should raise awareness of these Guiding Principles with relevant senior staff, such as staff involved in the development of policies, procedures and practices.

Financial institutions should advocate and raise awareness of accessibility issues and the existence of these Guiding Principles with their business and also, where appropriate, make their e-commerce partners, who may be evaluating and deploying stronger authentication technologies, aware of the existence of these Guiding Principles.

It is important for there to be broad customer awareness of the financial institution's commitment to accessibility principles.

Financial institutions should promote awareness of authentication technologies and the availability of alternative accessible options to help customers with disabilities and older customers to become aware of those alternatives. For example, if tokens are deployed, customers may be unaware that voice-output tokens can be issued to customers who are unable to read the display on the standard-issue token devices.

Financial institutions should ensure that customers and relevant staff are aware that, as a 'fall-back', a reasonably equivalent human-based alternative should be available to assist people with a disability and older people to conduct their banking transactions.

Financial institutions should refer to these Guiding Principles in relevant banking information. For example, financial institutions could make available dedicated sources and formats of information for customers with disabilities so that they have clear information on how to access their banking services.

Some topics could include:

- Accessible Downloadable Site Documentation: To assist new customers, downloadable documentation and quick reference cards for the site should be available, and kept up-to-date when site structure is altered. These materials should be available in accessible formats.

- Provision of Information: All text-based information, including terms and conditions and policy documents, shall be in plain English and available in accessible formats.

- Auslan: Financial institutions may wish to incorporate Auslan video clips to inform and assist deaf customers who employ Australian Sign Language (Auslan).

Principle 9: Confidentiality of customer information

Financial institutions must ensure the confidentiality of information of customers with disabilities and older customers.

The rights of privacy of customers with disabilities and older customers should be recognised and respected, and financial institutions must comply with any relevant privacy legislation.

It is important for financial institutions to know their customer. To assist financial institutions understand the needs of their customers, with the consent of the customer, a financial institution should appropriately store the user requirements and access preferences of customers. For example, a financial institution should appropriately store details of a customer's disabilities or access needs in relation to using authentication technologies, such as whether the customer is eligible to use an alternative authentication arrangement or device or conduct banking transactions via a human-based alternative, authorised third party or support service.

Customers should indicate to their financial institution their user requirements and access preferences so that financial institutions can identify and put in place suitable arrangements. For example, a customer should be able to declare that they use a Braille reader and they would prefer correspondence and their banking account information and material in Braille format.

<u>Explanatory guidance on Principle 9</u>

Financial institutions must comply with relevant privacy legislation, including the Privacy Act.

Some key areas for financial institutions to consider as part of their approaches to collection and storage of customer information include:

- Is personal data collected? If so, what kinds of personal data?
- How is personal data collected?
- How is personal data stored?
- For what purposes is personal data used?
- How is personal data controlled?
- What regulations, standards or guidelines apply to the collection and use of personal data?

Customers should be able to gain access to information about personal data practices without unreasonable effort, including the financial institution's privacy policy. Financial institutions should consult the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("OECD Privacy Guidelines"). [See http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html]

Financial institutions should consider the implementation of settings profiles for a user, so that preferred settings, such as screen colour, font style and size, text or graphics layout, audio settings and other parameters, are linked to an account or user identification number. User profiles should include preferred methods of authentication.

Some benefits to keeping details of customer preferences include:

- Keeping a record of the user's preference of authentication technology;
- Facilitating automatic selection of authentication (e.g. shared secrets in place of token devices);
- Keeping a record that the customer may be using a screen reader or other access or assistive technology, which may assist human agents in better understanding and addressing customer inquiries and requests; and
- Providing statements and correspondence in a format that is accessible to the customer (e.g. Braille, email, large print).

Financial institutions may need to develop individual arrangements and contracts to support deaf, hearing or speech-impaired customers who choose to conduct their banking via the National Relay Service/TTY, since this means that an intermediary or third party is involved in the transaction process. This should be reflected in business rules.

The privacy of the customer in regards to any information regarding disabilities will be protected in accordance with the National Privacy Principles. Financial institutions should consult the Guidelines to the National Privacy Principles. [See http://www.privacy.gov.au/business/guidelines/index.html]

Principle 10: Security of transactions and transaction fees

Financial institutions should ensure customers with disabilities and older customers are not exposed to higher financial risks or costs as a result of the deployment of authentication technologies.

Security: Customers with disabilities and older customers should not be exposed to higher financial risks if they are unable to use a particular authentication technology. For example, if an alternative authentication technology or process is used by a person with a disability, and an unauthorised transaction occurs, the financial institution should respond to the incident in the same way as it would for a customer using the financial institution's standard authentication system.

Fees: Customers who are unable to use an authentication technology or process should not be financially disadvantaged for using an alternative accessible option. For example, if they need to speak with a human agent or if they need to utilise branch services to complete their transactions, customers with disabilities or older customers should not be subject to higher fees.

Explanatory guidance on Principle 10

Where the financial institution and the customer have agreed to use an alternative authentication technology or process for access, there should be no change in liability, even where an authentication process may be less secure than the authentication technology deployed for other customers. For example, if an alternative authentication technology is used by a customer with a disability or older customer, and an unauthorised transaction occurs, the financial institution should respond to the incident in the same way as it would for a customer of the financial institution's standard authentication systems.

Where the financial institution and the customer have agreed to adopt an alternative authentication technology or process for access, financial institutions should not charge customers with a disability or older customers additional fees for making alternative authentication technologies or processes available. For example, if a customer needs to speak with a human agent or if they need to use branch services to complete their transactions, customers with disabilities and older customers that have agreed an alternative with the financial institution, should not incur additional fees. In certain circumstances it may be unavoidable to charge a fee as the transaction occurs, if fees are charged by a financial institution, all efforts to refund those fees will be done in consultation with the customer or by prior arrangement with the customer.

Financial institutions should consider the personal needs and circumstances of their customers. Due to the average lower income of many people with a disability or older people, it should not be assumed that the customer has a mobile phone or a computer, and it may be expensive for the customer to travel to branches, such as taxi fares. Financial institutions should be cognisant of this when designing and implementing authentication technologies, or devising alternative ways for people with disabilities and older people to access their banking services and conduct their banking transactions.

Appendix 1: Access issues facing people with disabilities and older people

This appendix contains additional background information. It does not set out any requirements to be met by financial institutions choosing to adopt the ABA's voluntary Guiding Principles for Accessible Authentication. This additional information is particularly relevant for Internet banking.

Introduction

The Australian Bureau of Statistics (ABS) estimates that 20% of Australia's population (or approximately 4 million people) have a recognised and ongoing disability. An even larger proportion of the population may have general reduced ability associated with age. Some hidden disabilities (such as eye injuries or psychological dysfunction, including stress) can also make it difficult for people to use authentication technologies.

All users will benefit from well thought-out web page and website design, from clear language to presentation of the most appropriate information, based on user preferences and profiles.

Access issues relevant to people with particular types of disability are described below.

Sensory

People who are blind or vision impaired

People who are blind have a total or near-total loss of vision rely more heavily on information from other senses.

For some people who are blind it is an advantage if the directions for use are available in a range of formats including on audio tape, CD, online or in Braille.

For users who have reduced vision, on-screen and printed information should be available in large print format.

People who are vision impaired will benefit from uncluttered web pages and web pages which display important information without other visual distractions, such as flashing or moving text.

Users who are blind will benefit from labelled graphics, consistent navigation, meaningful link names, textual or audio descriptions of video content, and the ability to access information otherwise only available on paper.

Users who are vision impaired or colour blind will benefit from highlighting text as the cursor moves over it, good colour contrast on pages, use of cascading style sheets allowing them to override screen fonts and colours and avoidance of reliance on colour as the only means of differentiating information on a web page.

People who are Deaf or who have a hearing impairment

Hearing impairment usually affects only part of the range of auditory frequencies. In some cases it affects the whole range. The higher frequencies are usually lost first with age.

Deaf people have little or no hearing and are much more reliant on visual cues and information. Deaf people may use sign language with English as their second language.

Users who are Deaf or hearing impaired will benefit from clear, concrete language, visual and text equivalents for audio content on web pages, and sign language videos which explain services and processes.

People with a physical impairment

Mobility

Reduced function in the lower limbs - due to disease, accidents or age – often leads to poor mobility, which can result in the need to use mobility aids, such as crutches or wheelchairs.

Customers with mobility disabilities will particularly benefit from the convenience of electronic banking. Where electronic banking services are offered in public areas or within branches it is particularly important that they are located in an accessible area and within accessible reach ranges.

Dexterity

Reduced function in the upper limbs, as a result of reduced strength or coordination, can make the operation of keys, knobs, handles and everyday utensils extremely difficult. Unless carefully designed, electronic devices may be difficult or impossible to use by people with poor dexterity or grip.

Users with arthritis or reduced fine motor hand control will benefit from minimal reliance on mouse movements for navigation and selection. Greater use of direction keys may be required in preference to a mouse.

To assist users with reduced dexterity, all areas of the website should be accessible with a single slow mouse click within a large button. Older users often have unsteady hand and arm movements and are often unable to accurately position the mouse on a small area. They may also have reduced reflex skills, which prevent the double click movement from being easily made.

Reaching and stretching

Almost all manual tasks involve an element of reaching and stretching. People with musculoskeletal disorders such as arthritis have difficulty reaching and stretching. The extent of effective reach is often determined by the amount of force to be applied by the hand and the posture that is adopted.

Headstick and mouthstick users, and people who can use only one hand, may be unable to press more than one key at a time. Consequently, it should not be necessary to press two widely separated keys simultaneously in order to activate any features and facilities.

Information

People with a cognitive impairment

People with cognitive disabilities and brain injury sometimes have poor memory, poor processing time or difficulty with complex messages. If instructions and assistance are given in an appropriate way, difficulties caused by cognitive impairment can often be overcome.

Users with epilepsy will benefit from text that does not flash and minimal use of moving text, as would older users, users with vision impairments and new users.

People with age-related cognitive impairments include Alzheimer's disease and dementia can experience progressive intellectual decline, confusion, and disorientation. Individuals with dementia experience progressive loss of mental functions. The most perceptual and cognitive limitations can be categorised as:

- Memory limitations: difficulty recognising and retrieving information;
- Perceptual limitations: difficulty taking in, attending to, and discriminating sensory information;
- Problem-solving limitations: difficulty recognising a problem; identifying, choosing, and implementing solutions; and evaluating outcomes;
- Conceptualising limitations: trouble with sequencing, generalising, categorising, cause and effect, abstract concepts, and comprehension; and,
- Language limitations: described separately in the following section.

Individuals with perceptual and cognitive limitations generally benefit from simple displays, clear language, simple obvious sequences, and cued sequences.

These individuals have difficulty understanding audio instructions, using written or electronic documentation, using automated systems, and/or using visual displays, depending on the type of limitation. Methods of improving designs to make them more accessible to this population include the use of voice prompts, increased size of print, simple fonts, high contrast, labels with icons or graphics, and progress displays.

People with a language or speech impairment

Language impairment and speech disabilities may result in difficulties using electronic banking systems. Pronunciation difficulties, fluency or loudness are the most common manifestations. These may be a problem where speech-input technologies or devices are used.

People with an intellectual disability

People with an intellectual disability will generally benefit from banking systems that use clear instructions and language and that are supplemented by face to face assistance when necessary.

The primary reason for knowing someone's "type" or "level" of intellectual disability is to identify suitable ways of providing support. Therefore, the "levels" are described according to the support needs of the person:

- The characteristics of support for people with intermittent support needs would be: episodic, not ongoing, every now and then depending on what's happening for that person. For example, support may be suitable at times of significant change, such as when someone registers for a new banking system. However, support is not required on a daily basis for the whole of someone's life.

- The characteristics of support for people with low or limited support needs are: minimal support is provided on an ongoing basis.

- The characteristics of support for people with medium or extensive support needs are that more substantial amounts of support are provided on an ongoing basis.

- The characteristics of support for people with high or pervasive support needs are that this support is ongoing and provided for all daily living activities, including all personal care and self maintenance activities (such as bathing and eating).

The access needs of people with an intellectual disability have to be recognised in the provision of banking services. The Guiding Principles seek to simplify processes that will help people with minor intellectual disabilities.

However, the Guiding Principles rely on the presumption that people provided with banking services have the capability to use those services without being in breach of the conditions of use that govern account operation. This requires as a minimum the ability to understand their rights and obligations, PIN security and usage, and the ability to correctly recognise transaction amounts presented for authorisation. Any lesser requirement might expose people with higher support needs to exploitation.

Appendix 2: Glossary

Key definitions

Authentication

There is an accelerating trend, both in Australia and overseas, to move beyond conventional single-factor methods, such as online usage of a user ID and password, for the purposes of verifying a customer's identity.

'Authentication' is the process of confirming the identity of a customer and verifying authority and access privileges, or validating a party authorised to communicate with a computer or computer program or with another user or customer, or proving the integrity of specific information.

'User authentication' is confirmation of the identity of their user or party authorised to communicate with a computer or computer program, or with another user.

Authentication can be performed either at the session level or transaction level, or both. 'Session authentication' allows the authenticated user to perform one or more transactions within a given session without the need for further authentication. 'Transaction authentication' requires a session authenticated user to undergo stronger authentication for each transaction in the session, in order to lower the security risk.

'Stronger authentication' refers to any authentication strategies considered stronger than conventional single-factor authentication, such as two-factor, multifactor, strengthened single factor and anti-keylogging strategies.

Existing authentication methodologies involve three basic "factors":

- Knowledge based factor '1st factor': something the user 'knows' (e.g. password, PIN). The first level of authentication consists of a minimum of two or more methods, where at least one of these factors is considered a 'shared secret';

- Possession based factor '2nd factor': something the user 'has' (e.g. ATM card, smart card). The second level of authentication consists of 1st factor and one or more methods involving a 'device';

- Biometric based factor '3rd factor': something the user 'is', or a behavioural characteristic (e.g. a biometric characteristic, such as a fingerprint, retinal scan, hand-writing, keyboarding patterns). The third level of authentication consists of 1st factor or 2nd factor and one or more methods involving a 'characteristic'. For example, the use of a user ID and password is single-factor authentication (i.e. relying on 1st factor credentials something the user knows); whereas, an ATM transaction requires two-factor authentication, being both 2nd factor something the user possesses (i.e. the ATM card) combined with 1st factor something the user knows (i.e. PIN).

A multi-factor authentication methodology may also include "out-of-band" controls for risk mitigation. Use of SMS-password or tokens are examples of an out-of-band strategy, because the information is conveyed to the user via a different channel to the channel being used for online banking.

Two-Way Authentication

In addition to a financial institution seeking to reliably identify and authenticate the customer, increasingly there are situations where a financial institution also needs to authenticate itself to the customer, or the customer's computing environment, in order to minimise incidences of 'phishing' and other account hijacking attacks.

This may be through the use of some kind of public key infrastructure, or it may be via a shared secret approach. For example, during enrolment/registration, the customer may have selected an image from a gallery, which is presented to the customer to 'prove' that it is the real banking service the user is connecting to. Use of images in this way could lead to access problems for people with vision impairments, unless those images used are clearly labeled with alt-text, etc. Alternatively, a gallery of sounds or musical samples could also be employed to address the visual-centric nature of shared secrets for two-way authentication.

Other terms used in the Guiding Principles

Authorised third party – includes someone that has been given lawful authority by a customer to act as their agent and perform the functions or duties as agent or in the best interests of the customer, either on a permanent basis or transaction/session specific basis. A third party may be authorised via a Power of Attorney or other formal authorisation, agreement or arrangement.

Biometric authentication – this term refers to technologies that measure and analyse human physical and behavioural characteristics for the purposes of verifying a person's identity. For example, physical characteristics including fingerprints, eye retinas or irises, facial patterns, hand measurements, voice recognition; or behavioural characteristics including signature or typing patterns. Some biometric traits share physical and behavioral aspects.

Internet banking – includes web content and applications as well as transaction services.

Plain English – language that is written as clearly and simply as is appropriate for the content. Clear and simple writing will aid all users, especially those with cognitive, learning, and/or reading disabilities. This should not discourage the writer from expressing complex or technical ideas. Using clear and simple English also benefits people whose first language is not English, including those people who communicate primarily in sign language.

Screen enlarger – (also termed 'screen magnifier') a piece of software that enables the user to enlarge computer screen print and graphics. Such software has features including zooming into specific screen content, tracking highlighting and mouse pointers and adjusting on-screen colours to enhance readability.

Screen reader – the term used to describe software designed to "read out" (or present in Braille) the contents of a computer screen for use by a person who is blind, vision impaired or who has a reading disability. Screen readers are available for MSDOS, Microsoft Windows, the Macintosh and some Unix platforms. Screen readers usually work hand-in-hand with a speech synthesiser or Braille display device in order to present computer information in an accessible format.

User Interface – the term used to describe the methods by which people and technology interact. User interface includes the output and input formats that programs generate and recognise. Depending on the user interface design of equipment, devices and software can be easy, difficult or even impossible for various groups of people with disabilities to access.

W3C - The World Wide Web Consortium (W3C) develops interoperable technologies (specifications, guidelines, software, and tools). The W3C was created in October 1994 to lead the Web to its full potential by developing common protocols that promote its evolution and ensure its interoperability. Organisations located all over the world and involved in many different fields join W3C to participate in a vendor-neutral forum for the creation of web standards. W3C has earned international recognition for its contributions to the growth of the Web.

WAI – Web Accessibility Initiative - a domain of the World Wide Web Consortium (W3C) charged with developing recommendations for accessible web design. It has several sub-committees that are looking at guidelines for web authors, browser manufacturers and web design and testing tools.

Web Accessibility – a philosophy of website design which endeavours to make a site as easy and effective to access for the widest possible range of potential users, irrespective of their limitations and capabilities, their location, equipment or bandwidth.

Other technical terms to be found in this document conform to W3C usage. A W3C glossary may be found at http://www.w3.org/.

Appendix 3: References

Documents which have influenced the development of the Guiding Principles include:

- *Industry Standards on Accessibility of Electronic Banking*. Australian Banking Association (2002) http://www.bankers.asn.au/Default.aspx?ArticleID=344

- *Online Authentication Guidelines*. Australian Banking Association (2005) (restricted circulation)

- *Background Paper: Forging a Balance between Banking Authentication Approaches and Accessibility by People with Disabilities*. Tim Noonan Consulting for the ABA (2006) (restricted circulation)

- *Universal Design Principles.* Centre for Universal Design. http://www.design.ncsu.edu/cud/

- *A Brief Introduction to Disabilities.* Trace Centre. University of Wisconsin-Madison. http://trace.wisc.edu/docs/population/populat.htm

- *Guidelines for the Design of Consumer Products to Increase Their Accessibility to People with Disabilities or Who Are Aging*. Working Graft 1.7 Trace Centre. University of Wisconsin-Madison. (1992) http://trace.wisc.edu/docs/consumer_product_guidelines/toc.htm

- World Wide Web Access: Disability Discrimination Act Advisory Notes. Version 3.2. (2002) HREOC. http://www.hreoc.gov.au/disability_rights/standards/www_3/www_3.html

- Web Content Accessibility Guidelines 1.0. W3C. (1999) http://www.w3.org/TR/WAI-WEBCONTENT/; http://www.w3.org/TR/WCAG10/full-checklist.html

- *Working draft of Web Content Accessibility Guidelines* 2.0. W3C (2007) http://www.w3.org/TR/WCAG20/

- *Accessible E-Commerce in Australia: A discussion paper about the effects of electronic commerce developments on people with disabilities*. Blind Citizens Australia (1999) http://www.bca.org.au/ecrep.htm

- *Draft guideline for user-friendly payment terminals*. Dutch Federation of the Blind and Partially Sighted and the Dutch National forum on the payment system.

- *Guidelines for the Design of Accessible Information and Communication Technology Systems.* Tiresias. http://www.tiresias.org/guidelines/index.htm

- *An Overview of Smart Card Accessibility*. The National Disability Authority (Ireland) http://www.nda.ie/cntmgmtnew.nsf/0/A0519A628DAD92A48025715A004A14C0/$File/Draft_Smart_Card_Accessibilty_Overview.doc