



Online Authentication Trends: 2007

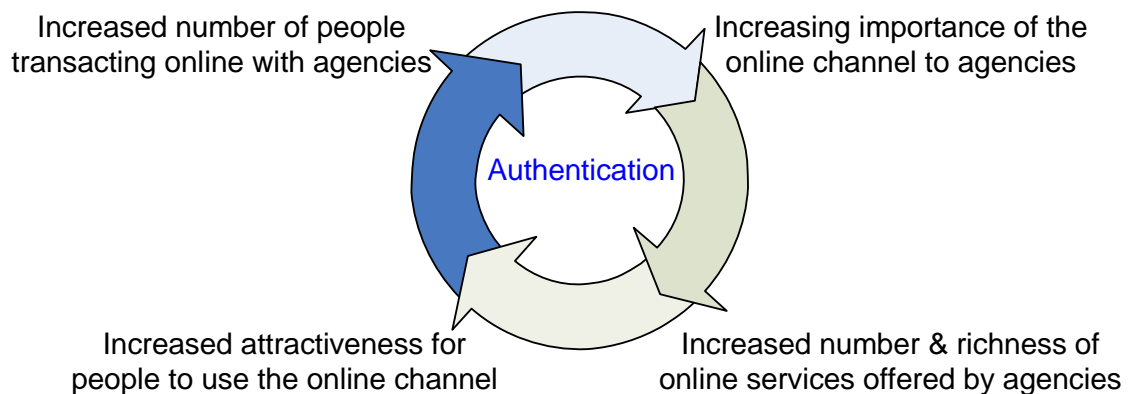
All-of-government Authentication Programme

Introduction

This report looks at global trends in online authentication from the perspective of New Zealand government agencies. These trends will influence our collective journey as we seek to leverage the online channel and Internet technologies to provide benefits to people, businesses, and government as a whole.

The focus in this report is on online authentication trends that have gained importance over the past year and look likely to be a major influence in the coming years. We have distilled the trends into six major categories. Not an easy or objective task considering that the online authentication space is currently in a period of rapid change.

Authentication can prime a virtuous cycle in which an increasing number of people have the confidence to transact online with government agencies, leading to increasing importance of the online channel for agencies. In turn, this will encourage agencies to increase the number and richness of online services offered, increasing the attractiveness of the online channel for people. The result is a self-reinforcing cycle of increasing people transacting online.



Alternatively, a failure to respond appropriately to authentication issues risks priming a vicious cycle of decreasing confidence, decreasing importance, stagnation (at best) of the number of services available over the online channel, and decreasing incentive for people to engage with the channel.

The Internet offers agencies a once-in-a-generation opportunity to deliver more coordinated, more accessible, more networked, and more trustworthy services to businesses and people. This is a real opportunity for government to meaningfully deliver on strategic goals articulated in the NZ Digital Strategy, Development Goals for State Services, and the E-government Strategy. A critical foundational requirement to benefit from this opportunity and help achieve government's transformational goals is online authentication.

We hope that you will find this report useful and welcome your comments and questions. Our email address is authentication@ssc.govt.nz.

Vikram Kumar

All-of-government Authentication Programme, State Services Commission

www.e.govt.nz/services/authentication

Summary of Trends and Action Points for Agencies

The Death of Passwords

There was a sense that 2006 was, finally, the tipping point for the demise of passwords for online services that have moderate or high security requirements. There are now viable alternatives with two-factor authentication solutions spanning a wide range of price points, form factors, and strengths.

Action Point for agencies: Conduct a high quality risk assessment of online services and, where the risks are found to be moderate or high, introduction of an appropriate two-factor authentication solution is recommended.

Identity's Third Wave: User-centric identity

In the past year the Third Wave of Identity has developed into a full-fledged wave. The characteristics of this user-centric identity framework includes user control, consistent experience across websites, protection of privacy, interoperability, multiple roles for people, multiple identity/attribute providers, and increased security.

Action Point for agencies: Agencies need to consider what the paradigm-shifting nature of user-centric identity means for them and respond. The future framework puts service users at the centre, using online services from multiple agencies and in control of the authentication exchange.

Old Scams, New Channel

In the past year or so, organised crime mobs have cemented their domination of the global cybercrime industry. As the New Zealand government steps up using the Internet and provides online services that have greater financial and reputational risks, it is inevitable that it will attract the attention of the Internet Mafia.

Action Point for agencies: Agencies need to work collectively to tackle this menace and maintain peoples' trust in the online channel at all-of-government and all-of-New Zealand levels.

Authentication is not just Identity alone

The moves towards user-centric identity and the rise of Web 2.0 has given rise to a trend for verifying information about a person online beyond just unique identity. For agencies there are many times when it is important to know a person's attributes authoritatively and online (in addition to the identity of the person uniquely).

Action Point for agencies: Agencies should widen their understanding of authentication to be the online, real-time verification of a person's or organisation's attributes, typically used for determining authorisation and/or entitlement, and not unique identity alone.

Authentication gets Dynamic

A trend is emerging with some service providers taking an approach that the risk from people accessing online services from their normal computer should only require a low strength of authentication. They therefore advocate that the type (strength) of authentication required should be dynamic rather than the same across the board.

Action Point for agencies: For agencies considering dynamic authentication, caution is advised until this approach proves itself. On the other hand, if and once it does, dynamic authentication may be a useful addition as a part of a wider, integrated suite of authentication services.

SAML 2.0 the Default Choice

All three of the major open standards for identity federation have come together in Security Assertion Markup Language (SAML) v2.0. Over the past year, there have been several commercial off-the-shelf and open standards' software products introduced.

Action Point for agencies: When developing or re-developing identity management systems, agencies should consider SAML 2.0 as the default choice in implementing identity management messaging online.

Online Authentication Trends

The Death of Passwords

Reports of the death of passwords have been greatly exaggerated in the past. Bill Gates put passwords in the spotlight when he famously [predicted the demise of passwords](#) at the 2004 RSA Conference.

The reality is that the use of passwords is at equilibrium. People don't like to remember a large number of passwords but they are easy to use and ubiquitous. So people devise ways to manage them, from simply using the same password or a minor variation of it everywhere to writing them down or saving them in a file. On the other hand, service providers find it easy and economical to use passwords for authentication and try to find ways to minimise the downsides, such as help desk costs in re-setting passwords.

But the equilibrium is becoming increasingly unstable and there was a sense that 2006 was, finally, the tipping point. Service providers and people alike are now increasingly acknowledging that passwords provide only a minimal level of security online.

Passwords have several flaws. One example is that the stronger the service providers try to make them, such as specifying a requirement for multiple character sets or increased frequency of change, the more likely service users are to write them down or devise other ways to adapt that weaken the strengthening efforts. There are other flaws with passwords including the limits of human cognitive capabilities in remembering many, many application-username-password sets and the relative ease in extracting passwords using a variety of social and technical vulnerabilities.

The approach to security online must therefore assume that people can and will give away their passwords relatively easily. A large number of online services are under-protected and vulnerable as a result. There are now viable alternatives with [two-factor authentication](#) solutions spanning a wide range of price points, form factors, and strengths.

And, not only do these alternatives provide more security than passwords, people are beginning to ask for better protection online. Most major and second-tier banks in New Zealand [now offer two-factor authentication](#) to their online banking customers. Banks have reported greater than anticipated customer uptake and a reduction in fraud.

The weaknesses of passwords are causing regulators to step in. A prominent example is the [requirements imposed by FFIEC](#) (Federal Financial Institutions Examination Council) on US financial institutions. These requirements labelled the use of passwords alone as inadequate and required "multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks".

Deployment of two-factor authentication extends well beyond banks. VeriSign has launched a service called [VeriSign Identity Protection](#) (VIP) that allows customers to use the same [token or credential](#) across all VIP-enabled sites. Early customers include heavyweights such as eBay, PayPal, and Yahoo. In Australia, VIP is now [offered through Australia Post](#), a step closer to two-factor authentication being marketed to customers direct as a mass market consumer product.

With the use of two-factor authentication now successfully spreading from the business/enterprise markets (where it originated) to consumer markets, the demise of passwords for moderate or high security requirements is nigh. And yes, Bill Gates again used the 2006 RSA Conference to predict that the [end of passwords is in sight](#). This time around more people share the same vision.

Action Point for agencies: Conduct a high quality risk assessment of online services (using the standard [AS/NZS 4360](#)) and, where the risks are found to be moderate or high, do not rely on passwords alone. Introduction of an appropriate two-factor authentication solution is recommended, supported by a layered security approach (such as adequate monitoring and reporting).

Identity's Third Wave: User-centric identity

In the past year the Third Wave of Identity developed from being a small ripple to a full-fledged wave, sweeping through the online authentication world.

The First Wave of identity management was directories to abstract identity from applications. The Second Wave saw large scale but silo-focussed identity management deployments within the enterprise. The Third Wave takes identity management to Internet scale and puts service users rather than service providers (agencies) in control. The characteristics of the Third Wave of user-centric identity also includes consistent experience across websites, protection of privacy, interoperability, multiple roles for people, multiple identity/attribute providers, and increased security.

New Zealand's approach to online authentication, based on [policy and implementation principles](#) approved by Cabinet in 2002, pre-dates the Third Wave but is fully aligned with it.

There were two launches during the past year that really typify the Third Wave- [Windows CardSpace](#) and [OpenID](#).

First, Windows CardSpace which is software running on a person's computer that provides a more intuitive interface to understand, manage, and confirm the person's digital identity to service providers. Windows CardSpace is shipped with Microsoft's new operating system, Vista, and as an optional add-on to Windows XP, making it available to millions of people around the world. With the launch of Windows CardSpace, Microsoft is putting into practice lessons learnt from the failure of an earlier online identity initiative called Passport as well as a more user-centric architecture called the [Identity Metasystem](#).

Secondly, OpenID which is based on the concept that people can identify themselves on the Internet the same way websites do, with a [URI](#) (also called a URL or web address). With OpenID, people log in with their password or other credential at a third party's website, called an Identity Provider. People are also able to control what pieces of information can be provided by their Identity Provider to a service provider, such as their name, address, or phone number.

OpenID has its roots in blogging and a need to protect a person's reputation online. This has led to some weaknesses in the system, especially a lack of linkage to a person's real identity, and it is prone to [phishing](#). However, OpenID is rapidly gaining traction in the social networking arena with even Bill Gates using his last appearance at RSA Conferences in 2007 to announce that [Windows CardSpace will support OpenID](#).

There were many other developments in the past year that herald the arrival of user-centric identity to the mass global market. These initiatives will fundamentally shape the evolution of online authentication over the next few years.

Action Point for agencies: Agencies need to consider what the paradigm-shifting nature of user-centric identity means for them and respond. The current online authentication framework is a single agency providing online services to multiple service users with the agency in control of the authentication. The future framework is the other way around, with a service user using online services from multiple agencies and the user in control of the authentication. This also implies the need for greater joined-up online services.

Old Scams, New Channel

An infamous US bank robber of the 1930s, [Willie "Slick Willie" Sutton](#), when asked why he robbed banks replied, "Because that's where the money is." One of Slick Willie's trademarks was to rob banks in broad daylight in disguises as varied as a policeman, a messenger, and a maintenance man. This was at a time when the Mafia were consolidating their networks across USA in the Prohibition-fuelled days of lawlessness.

His story is a good parallel for what's happening on the Internet now. The Internet gives the Slick Willies of the world a global reach, without putting them in physical danger. The

complexities of investigating and prosecuting cross-jurisdictional crimes makes the Internet a perfect channel for scams and attacks based on the age-old human frailties of greed, fear, guilt, temptation, etc.

[MSNBC reported](#) five years back that 2002 was the year criminals took over the Internet from amateur, fame-seeking, teenage graffiti artists. But it is only in the past year or so that organised crime has cemented their domination. A eWeek article talks about the Web Mob having [a level of sophistication and brazenness](#) that is "frightening and surreal."

The article describes over-educated and under-employed hackers in Eastern Europe, Asia, and Latin America selling their skills to eager buyers in a truly global industry. There is a growing trend for targeted crime online, even as the old problem of spam based on a fractional response from millions of emails remains rampant. Thus the dramatic rise in the past year of malware such as [rootkits](#), [Trojans](#), [spear phishing](#), [keyloggers](#), and [botnets](#).

The cybercrime industry is now organised in a similar way to the drug-trade with the same hierarchal levels of bosses, regional lords, traffickers, dealers, producers, and "mules". A report by McAfee details how a [new generation of criminals](#) are now controlling cybercrime. The war on cybercrime is likely to be as difficult, costly, and time consuming as the international war on drugs.

The [online equivalent of extortion](#) is to launch a [denial of service attack](#) which can force the victim to completely shut down if they don't comply with the Mob's demands. In these cases, unlike that of Slick Willie, the good guys aren't always winning. Many successful attacks have been launched against [online betting sites](#) though there are others where it was [more personal](#) or to make a [political point](#). A few websites have [managed to win](#) and hard lessons are being learnt on what works and what doesn't.

New Zealand has been fortunate in being spared the worst of these scams and attacks. Even then, TVNZ's [Fair Go programme reported](#) that thousands of New Zealanders a year are victims of foreign lottery scams.

With online crime becoming global and organised, there are no grounds for complacency in New Zealand. As government steps up using the Internet and provides online services that have greater financial and reputational risks, it is inevitable that it will attract the attention of global criminal mobs.

There may be a point in the future where the defence of valuable Internet assets is more difficult than what most agencies are comfortable with in handling themselves. At that time, security as a service will become valuable and will integrate more richly into agencies' infrastructure.

Action Point for agencies: There is a lot that agencies can and should do to prepare themselves and their customers for increased attention from the Internet Mafia. At the same time, agencies need to work collectively to tackle this menace and maintain peoples' trust in the online channel at all-of-government and all-of-New Zealand levels.

Authentication is not just Identity alone

Explanation of this trend requires clarification on the term "identity". In many overseas jurisdictions, identity in relation to people is defined as a quality or characteristic a person has. This is intended to be very wide and covers all types of information about people.

In New Zealand, we refer to these as "attributes" of the person and define "identity" more narrowly as the uniqueness of the person. A sub-set of attributes ("identity data") serves to describe that uniquely identified person. For example, in New Zealand, the person's name, date of birth, place of birth, and sex are identity data while address, role, presence/absence on a public register, agency identifier, etc. are all considered to be attributes.

The trend towards user-centric identity referred to earlier and the rise of [Web 2.0](#) has given rise to a trend for verifying the attributes or information about a person online

("authentication") beyond just unique identity. For example, a person's reputation in online auction sites such as [TradeMe](#) is far more important in buying/selling than a knowledge of who the person really is (name, date of birth, etc.). Reputation is also critical in other user-generated content such as blogging. So important in fact that OpenID, referred to earlier, relies on it to create the person's digital identity.

For government agencies there are many times when the unique identity of the service user requires to be known, for example when a person applies for a student allowance or loan. However, there are many other times when it is more, or at least equally, important to know an attribute of the person rather than the person uniquely. For example, if the National Library provides discounts to students accessing certain digital content, it is more important for National Library to be assured that the person is a student (an attribute) rather than the unique person (name, date of birth, etc.).

Some overseas examples of this trend include the need to know the age of people joining social networks such as [MySpace](#) to [protect underage children](#), using group reputation to determine the interest rate to be charged for [borrowing money online from peers](#), and [allowing university students to purchase books](#) from independent book stores at discounted prices.

Within the New Zealand government context, there are a number of attributes that are authoritatively known to an agency which are of interest to other agencies. Examples include the person being a student, a Director of a particular company, permanent resident, licensed building practitioner, owner of a particular house, IRD number, worker on a particular child's case, etc.

While agencies have been obtaining attributes about people or businesses using traditional, non-online channels, typically to help determine authorisation and/or entitlement, the trend is to get these attributes online, in real time, at the request of and under the control of the user.

Action Point for agencies: Agencies should widen their understanding of authentication to be the online, real-time verification of a person's or organisation's attributes, not unique identity alone. Agencies should consider what attributes they can authoritatively verify about people or organisations to other agencies online and, at the same time, how they can use attributes received from other agencies online.

Authentication gets Dynamic

The standard approach for service providers has been to decide on a type of authentication, for example passwords or [tokens](#), and require every service user to present that credential each time the person wants to access the online service.

However, some vendors argue that the risk from a person accessing the online service "normally" should only require a low strength of authentication and therefore authentication requirements should be dynamic rather than the same across the board. For example, a person accessing online banking from within New Zealand using the computer that he normally does should only need a password to logon. The same person accessing online banking from a computer not in New Zealand should require a stronger logon type, say a token, or provide additional information, e.g. answers to "life questions".

This alternative approach is being advocated by vendors, particularly those that have made acquisitions of companies that provide the software for doing "dynamic authentication" or "adaptive authentication". It is essentially based on using the service user's computer as the second factor to achieve two-factor authentication and therefore suffers from obvious limitations when it comes to flexibility of access.

A prominent example is [RSA's offering](#) based on the [purchase of Cyota](#) which operates transparently behind-the-scenes and does a real-time risk assessment. In the event that a pre-determined risk threshold is crossed based on various pre-defined parameters, the

service user is prompted for additional information, out-of-band confirmation (for example, a phone call), or a stronger logon credential such as a token.

Critics are dismissive of this alternative approach. They believe that the additional security offered over plain passwords is insufficient. These critics also claim that service providers adopting this approach use the excuse of providing better customer experience to avoid the costs of implementing proper security that their service users require.

On the other hand, vendors believe that dynamic authentication as a part of a wider, integrated suite of authentication services provides a real alternative to requiring every service user to use two-factor authentication every time people want online access. Several financial institutions have adopted this approach in response to the FFIEC requirements mentioned earlier.

Action Point for agencies: For agencies considering dynamic authentication, particularly as a way of implementing two-factor authentication for service users usually accessing online services from the same computer, caution is advised until this approach proves itself. On the other hand, once this alternative approach proves itself, it may be a useful addition as a part of a wider, integrated suite of authentication services.

SAML 2.0 the Default Choice

When considering online authentication beyond the enterprise or agency, for example single sign-on or identity assertions at a sector or all-of-government level, the issues of consistency and interoperability are of great importance. Adopting open standards is therefore recommended over tightly-bound approaches such as [Web Service \(WS\)-Federation](#) which, even though royalty-free licences to implement the specifications are available, tend to work best with proprietary stacks such as Microsoft's.

In the past, there have been several open standards that have been adopted globally. The three major ones were [SAML v1.1](#) (Security Assertion Markup Language) from [OASIS](#), [Liberty Alliance's Identity Federation Framework \(ID-FF\) v1.2](#), and [Shibboleth](#). All three of these came together in March 2005 in [SAML v2.0](#).

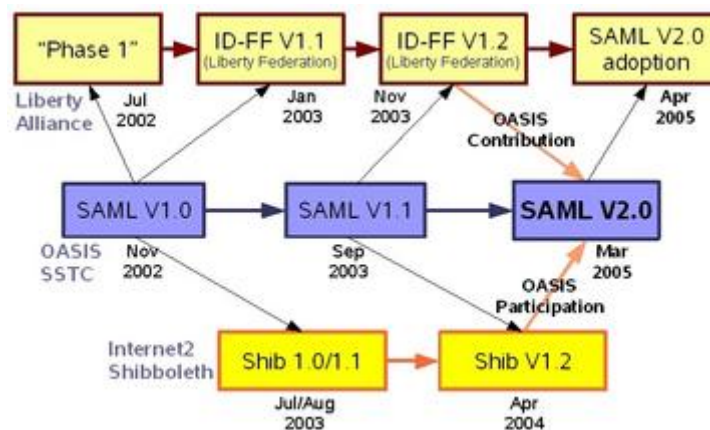


Illustration from [Liberty Alliance](#)

Over the past year, there have been several commercial off-the-shelf and open standards' software products introduced that implement SAML v2.0. This makes SAML 2.0 the default open standards choice in implementing identity management (including authentication) messaging online. Since SAML 2.0 is incompatible with SAML 1.1 and 1.0, going direct to v2.0 is recommended for new developments/re-developments.

Liberty Alliance members from the UK, US, Denmark, and Finland made a presentation at the 2007 RSA Conference confirming publicly their view that [SAML 2.0 is the standard of choice in the public sector](#).

However, the story of evolution and convergence/divergence of the standards is not over by any means, especially in respect of web services.

Action Point for agencies: When developing or re-developing identity management systems, agencies should currently consider SAML 2.0 as the default choice in implementing identity management messaging online.