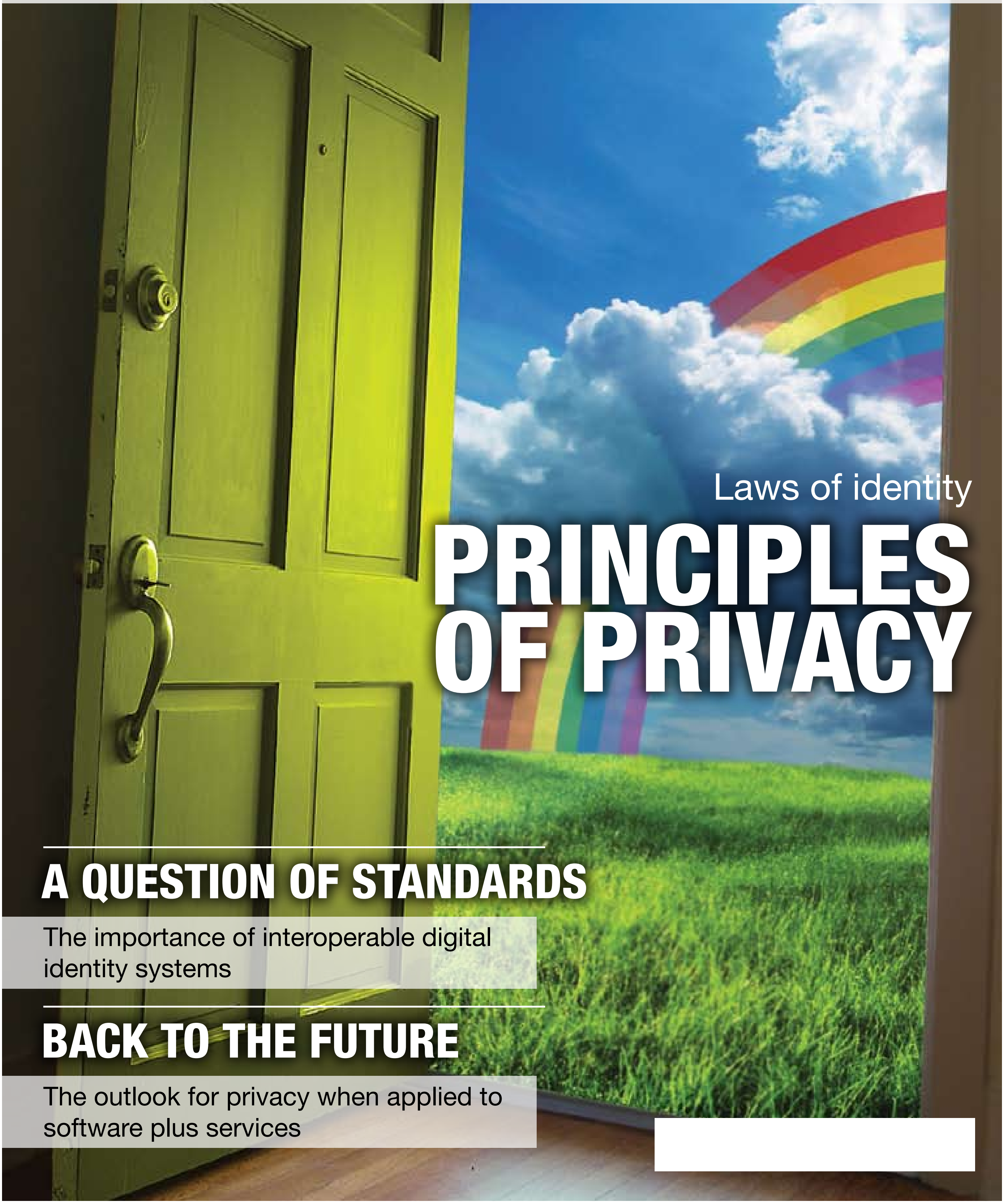
theARC magazine

ISSUE 03

SOFTWARE + SERVICES



Laws of identity

PRINCIPLES OF PRIVACY

A QUESTION OF STANDARDS

The importance of interoperable digital identity systems

BACK TO THE FUTURE

The outlook for privacy when applied to software plus services

Welcome to issue 03

When the Internet was designed the notion of identity theft was inconceivable and we have lived with the results of that situation ever since. Phishing, fraud, identity theft and numerous criminal activities have become the norm and we all know somebody who has suffered an Internet identity scam of one sort or another.

Indeed, as we walk the streets of our towns and cities it is easy to determine when something seems wrong or unsafe. There are cues and guides we absorb and evaluate without even thinking about. However, on the information superhighway no such cues or guides exist.

There are standards for IP, TCP, HTTP and so on, but there is no single unifying standard for identity and this lack of a formalised system has resulted in a hotchpotch of ad-hoc one-offs to address the problem. The vast majority of sites request a username and password, but there is no consistency about the way these secrets are asked for. Some even believe that we have got to the stage where a user will type his secret passwords into just about any web page that asks for it.

As web technologies permeate the enterprise, similar problems are encountered inside an organisation. Then, when this enterprise connects with others, the plethora of user accounts and passwords result in so-called password fatigue. With many of these sites being accessible from the Internet, clever criminals have the opportunity to easily phish valid, usable enterprise passwords from unsuspecting users.

Each system developed by different organisations deploys varying standards or custom code and proprietary protocols. Then, as more enterprise systems are integrated with one another across organisational boundaries, software engineering work has to be done to one or more of these systems to make them work together. With additional organisations entering the mesh of systems things become even more complicated.

As enterprises decide to run more of their applications off-premise, hosted, or in the cloud, these integration problems become even more difficult to solve in the traditional way – as a series of ad-hoc one-offs. What is needed is an identity system that runs among the existing tiers of the Internet and deals with digital identity. It must also address the issues of the many identity token formats and make it easy for the users of such a system to know who and what to trust, so that they aren't fooled into giving away secrets to fraudsters.

This system should be valid and consistent inside and between businesses, as well as on the Internet when consumers and citizens connect to websites. This should be the case when accessing services in the cloud, within this and the enterprise. Until that day comes, cloud computing serves only to exacerbate the existing problem.

Of course, some very clever people have already been thinking about these dilemmas and answers already exist: from Linux, Mac and Windows on the client – to server products either released or soon-to-be-released from the likes of Sun, IBM, Microsoft, Novell, CA, RSA etc, on the cloud computing platform.

In this issue we aim to change the way you think about digital identity as we take a closer look at how this fits into the notion of software plus services.

Paul Mackinnon
Lead Identity Adviser, Microsoft UK

Steve Plank
Identity Architect, Microsoft UK

Questions or thoughts? Email: thearc@microsoft.com

Cover illustration: www.stokeripley.com

Contents

Additional Contribution from:
Koby Amedume: Platform Marketing Lead, Microsoft UK
Matt Deacon: Chief Architectural Advisor, Developer & Platform Group, Microsoft UK

The Arc magazine Software+Services is published on behalf of Microsoft Ltd by NGT Media Ltd. No part of this magazine may be reprinted or used without the publisher's written consent. **www.ngtmedia.co.uk**

Microsoft Limited, Thames Valley Park, Reading, RG6 1WG

Digital identity
The background

Unbeknown to most of us, as soon as the first application needed to distinguish one user from another the notion of digital identity was born.

However, it's only recently that we've begun to think about all this as digital identity and it wasn't until applications became connected via the Internet that almost everybody had to get a handle on the issue of Identity management.

With usernames and passwords coming out of their ears, those on the information superhighway soon found themselves targets of a new phenomenon known as identity theft.

Next came the idea of a series of computer networking standards covering electronic directory services and a vision of a world where all countries, network operators, companies, computers and users would be linked together through a huge directory system – the X.500 directory.

The idea was one of a large central repository that everybody and every resource was connected to – a utopian vision of perfection so-to-speak.

But of course, this had to be partitioned. One country would want to be responsible for its own citizens and resources after all. In addition, factions in countries that were at civil war both claimed to be authoritative for their country's entry in the directory and the directory placed considerable technical demands on computers that connected to it. Detractors and privacy lobbyists also lambasted it as a honey pot for criminals and totalitarian regimes that could put its citizens under surveillance. The result was that rather than a single worldwide directory, it spread and fragmented over different parts of the world becoming managed mostly by telecoms operators.

However, this technology was deployed with some success inside organisations and it was here that the idea of the 'enterprise directory' really started to take hold.

Yet, this too began to suffer similar problems as it turned out that no one company could ever manage to have all its users, applications, servers and services all housed in one large centralised directory. Other directories and databases would always spring up and consequently most enterprises to this day still have multiple logins for their users.

When Microsoft (MS) Passport was released its aims were laudable – to provide a large Internet-based authentication system so that if you were building an application, you could leverage it. Yet, dogged by the same problems from lobbyists and detractors it was only every really used for MS web properties.

Both x.500 and Passport tried to solve the problem by being all things to all people, but this ignored the requirements of the person whose identity was being managed. We as humans actually like dividing our lives in to different contexts.

Indeed, our lives obey an architectural principal called the 'pluralism of operators and technologies'. This is the idea that our real lives deal with many different forms of identity on a daily basis and we like this on the Internet. So, large centralised databases of identity are not the answer. The answer is to build systems that allow for multiple sources of identity – just like in our real lives.

The Enterprise has the same problems. Users with logins to multiple systems all have different password policies and different username formats. For them, trying to get an identity on one system understood by another is a major problem, with integration often proving difficult as they have issues attempting to share and reconcile data.

Many feel that what's needed is a solution allowing systems that use different standards to interoperate with each other – one that is device independent. This is the power of the Identity Metasystem which works in the cloud, on the Internet, inside and across enterprises. It embodies the notion of 'user-centric identity'.

JARGON...?

X.500
The X.500 was a standard for developing an electronic directory of people in an organisation so that it was part of a global directory available to anyone in the world with access to the Net. Such directories are referred to as 'white pages' directories.

Identity

Much has been made of 'claims-based Identity' and why it is important within the digital space. The Arc spoke to Steve Plank, Identity Architect, Microsoft UK, to find out more.

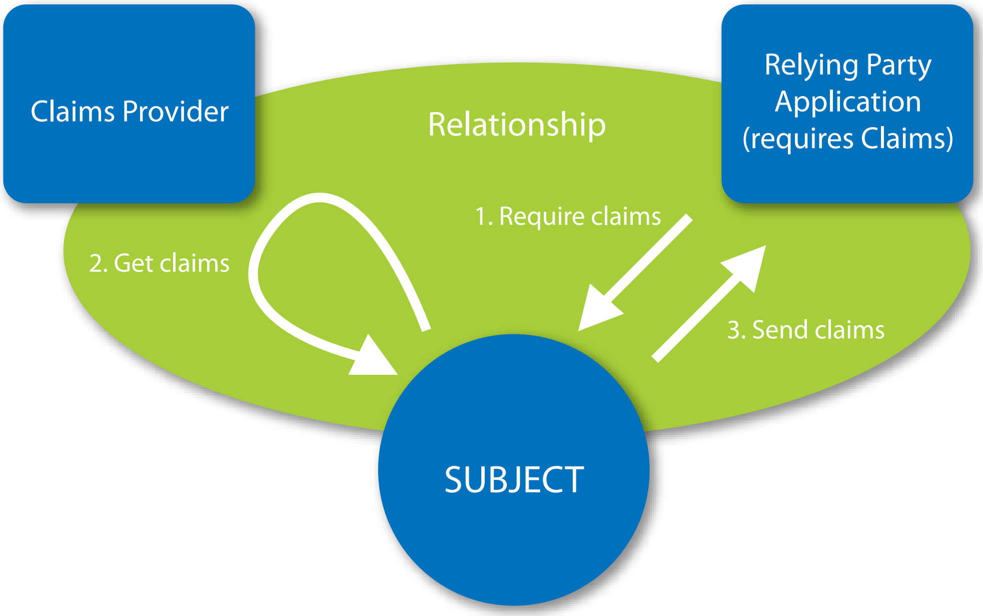
The science

A claim can be seen simply as a statement that one subject makes about another. It could be that you have blue eyes or have the National Insurance number 214356 for instance.

Such claims are normally packaged up as 'security tokens' and credit cards, video club membership cards, driving licences and bank notes are all examples of these. A bank note for example contains a claim – five pounds. This is what needs to be conveyed from buyer to seller – or in the parlance of digital identity, from the 'subject' to the 'relying party'. All other printing on the banknote is a collection of authenticity marks and the receiver checks these to ensure the note was genuinely issued by the Royal Mint. (see fig.1)

"The receiver can be said to be making a decision on whether they trust the bank note," says Plank. "They extract the claim 'value = five pounds' which is the data they need to enable them to provide you with the service you want."

figure 1



This means we can do the same thing electronically, moving claims about ourselves packaged into data structures called security tokens, and take these securely and privately from a company's network to a service running in the cloud.

"The service can then be assured that the token came from my company and make decisions on what data I can access based on the claims in the token," adds Plank. "It's a powerful but simple model."

This model can be thought of as the road network that links people together. Everybody who uses it agrees on a set of rules or 'protocols'. They all drive on the same side of the road and they all obey traffic lights. Everyone uses roundabouts in the same direction. This is the infrastructure that transports the vehicles (tokens) that contain the claims (people). There are various types of vehicles: trucks, taxis, vans and bikes. And there are all sorts of people: girls, boys, women, men, the old, and the young. The road network doesn't worry about the type of vehicle or its contents and allows these elements to work together in harmony. In identity circles we refer to the road network as the 'Identity Metasystem'.

However, the real power of the metasystem is in the fact that the transport layer is agnostic to the vehicle. In software terms this represents full interoperability.

In order for subjects to pass claims to a relying party, they must first retrieve them from a 'claims provider'.

"There is a pre-existing relationship between a claims provider and a relying party," explains Plank.

"Claims Providers create the tokens and put the claims in them and send them to the 'subject,'" he says. "This is the actual user who gets their claims from the provider and presents them to the 'relying party'. These tokens can be transparent to the identity metasystem and we can pass for example, a SAML token, an x.509 certificate or even a custom token containing claims about you."

So, for example, a website or application (relying party) requests you log-on and will express a set of claims it needs to access this service, claims providers you can to get them from, and a token format it understands. The subject (user) then selects a claims provider (Identity provider), proves who they are and sends them the security token (the data structure containing the claims they need to access this website or application).

"The user then passes those claims on to the relying party [application]," he adds. "It means you can separate identity data from the application data and manage both in a more meaningful way."

Plank says that Microsoft's strategy is to embed the claims-based identity model into Microsoft's entire product portfolio. An example of this is software the company has been building codenamed "Geneva".

# of digital identity

This consists of three parts.

Claims Provider	"Geneva" Server
Relying Party	"Geneva" Framework
Subject	"Geneva" CardSpace

Geneva Server (claims provider) allows users to expose an organisation's identities through industry-standard protocols, whilst Geneva CardSpace is the client software that allows a user to select the appropriate claims provider. There are others like DigitalMe for Mac and Linux and these interoperate with each other.

This, he says, means users can take information cards from a Mac and use them on a Windows computer in just the same way.

Geneva Framework (relying party) is a toolkit that developers use to build claims-based applications.

"This provides an interoperability layer that allows applications to consume tokens from other token providers, no matter what platform they are running on," says Plank.

"As we consider the idea of Software plus Services we can see how important this model is," he adds. "Microsoft's entire product portfolio is integral to the Software plus Services story."

There is also the Microsoft Federation Gateway which is hosted in the cloud. This communicates with enterprises using industry standard protocols and allows an organisation to 'federate' its internal identities with applications it has running in the cloud.

According to Plank, this gives a seamless experience to the user who simply clicks on a link and their identity is projected through federation technologies into the cloud.

"They aren't re-prompted for credentials, it's just as if the application is running on-premise," he says.

An example of this might be a company that decides to use Microsoft's Dynamics CRM online – an application which is hosted in the cloud. The user clicks the link on their desktop and the application opens up ready for them to use. The user doesn't need to know how it works, rather they just need to experience a feeling of the way things work when they run applications locally inside of the company network.

Information cards fit into this model by filling a space much in the same way as a credit card or frequent flyer card might identify you.

When you use a credit card in a shop, you authenticate with your PIN to the bank before a payment is released.

"Information cards use this metaphor which we are all very familiar with to do identity transactions on the Internet," says Plank. "Information cards are data artefacts that live on your computer."

Visually, these look a bit like the plastic cards in your wallet, don't contain any data, but can be used to get security tokens from claims providers.

"They give an experience to the user which is analogous to the one we're all used to: showing a card to somebody to get something," he adds.

Information cards are about more than just usability though. As they contain cryptographic material, it means the security of information like your password or your PIN is more highly protected. Users don't type a password into a web page. They type it into software on their computer and the cryptography ensures that only the issuer of the card can unscramble your password. This dramatically reduces the threat from phishing sites.

"The other nice by-product of this is that when you use information cards you go through a 'ceremony'. It's the same ceremony no matter what website or application you use," says Plank. "If one day, that ceremony is broken by a site trying to steal your data, you are alerted. Your senses are heightened and you become more circumspect.

"There are ethereal cues to danger in real life that are entirely missing from the Internet," he adds. "You never truly know when you are in danger on the Internet. Information cards, through their 'ceremony' add this property to your Internet interactions."

If you think about how Chip and PIN works there are strong analogues with the online world. When you type in your PIN, which is the equivalent of your password or smartcard/PIN on the Internet, you are in a private dialogue with the banking network. When they are happy that you are who you say you are, they release a payment to the shopkeeper.

"He never gets to see your secrets," says Plank. "It shows user-centric identity, ceremony and a very rudimentary notion of the identity metasystem. I believe when this is maturely adopted on the Internet in a few years time, it will be safer to buy something online using information cards than it will to buy something in a high street shop."

Microsoft's implementation of Information Card software is known as 'Windows CardSpace', with the next version currently codenamed 'Geneva' CardSpace.

"Take the example of a user logging in to the cloud-based application that we were talking about earlier," adds Plank. "What if the user was outside the company's firewall, say at home? Most home networks simply aren't run to the same security standards as a corporate network. So, to increase security, you could use Information cards to access the cloud applications when you are outside of the company network."

JARGON...?

SAML Tokens
Security Assertions Markup Language (SAML) tokens are XML representations of claims. They carry statements that are sets of claims made by one entity about another. In federated security scenarios, the statements are made by a security token service about a user in the system.

Geneva
The Microsoft code-named "Geneva" claims-based access platform allows developers and their customers to simplify user access with a single model that's open and interoperable.

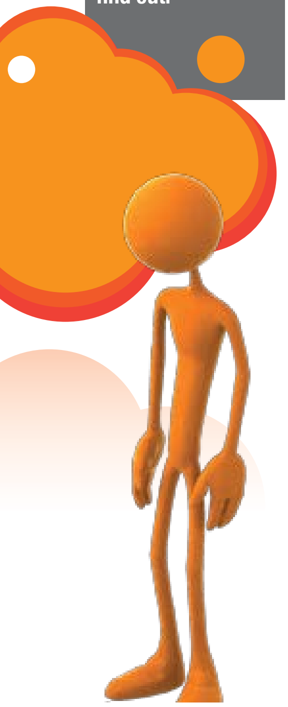
WS-Federation
WS-Federation is an Identity Federation specification. As part of the larger Web Services Security framework, WS-Federation defines mechanisms for allowing disparate security realms to broker information on identities, identity attributes and authentication.

WS-Trust
WS-Trust is a WS-* specification and OASIS standard that provides extensions to WS-Security, specifically dealing with the issuing, renewing, and validating of security tokens.

A question of standards

Standards

What it is about interoperable digital identity systems that make standards such an important part of the story? The Arc decided to find out.



Products that follow standards correctly become part of the standard wiring and power solutions that link systems together. In the UK we have 240 volt and 50Hz AC mains electricity. Our houses, offices and buildings contain wiring that conforms to those standards. Everything from the kettle we use for our morning coffee, to the washing machine and the phone charger we use adheres to that standard.

"Some years ago I accidentally plugged an American 110 volt computer into the UK supply," explains Craig Wittenberg, lead architect from Microsoft's Corporate Identity and Access Strategy team. "When I switched it on there was a loud bang, a puff of blue smoke and it stopped working."

It's clear we must agree on standards to convey identity information between endpoints that have the right properties to avoid repeats of the above in the fields of privacy, security and so on.

Wittenberg says that, for its part, Microsoft works closely across the industry with partners, competitors, customers and standards bodies to ensure that it makes sense to all of the players when standards go through revisions.

Talking about Azure, the new cloud platform offering from Microsoft, Wittenberg adds, "I think it's one of the great assets of Azure that you can buy an identity product from IBM, deploy it in to your organisation and use it to project your corporate identities into the Azure cloud to make it seem to the user that they are using an application on the local network. Without standards we'd never have been able to achieve that."

When 'Geneva' is released it will support the following two protocols of the Web Services Standards stack (WS-*): WS-Trust and WS-Federation. Wittenberg explains that it will also support the SAML Web single sign-on (SSO) protocol. In addition, there are the different token formats that need considering. The SAML protocol obviously supports the SAML token and he explains 'Geneva' will support SAML 1.1 and 2.0 tokens.

"The WS-Trust protocol is token agnostic," he says. "It isn't concerned with the internal structure of a security token. So you could for example convey an x.509 certificate or a Kerberos ticket inside the token.

"The 'Geneva' framework, that's the toolkit a developer would use, supports WS-Federation and WS-Trust," he adds. "The 'Geneva' CardSpace client supports the WS-Trust protocol."

Of course web browsers from any vendor are passive clients and this means they automatically have support for WS-Federation and the SAML WebSSO protocol. Browsers do not support WS-Trust directly, but if they have support for an active client such as CardSpace, the DigitalMe client for the Mac, and Linux or the Higgins selector that runs on a number of platforms, they can support WS-Trust that way.

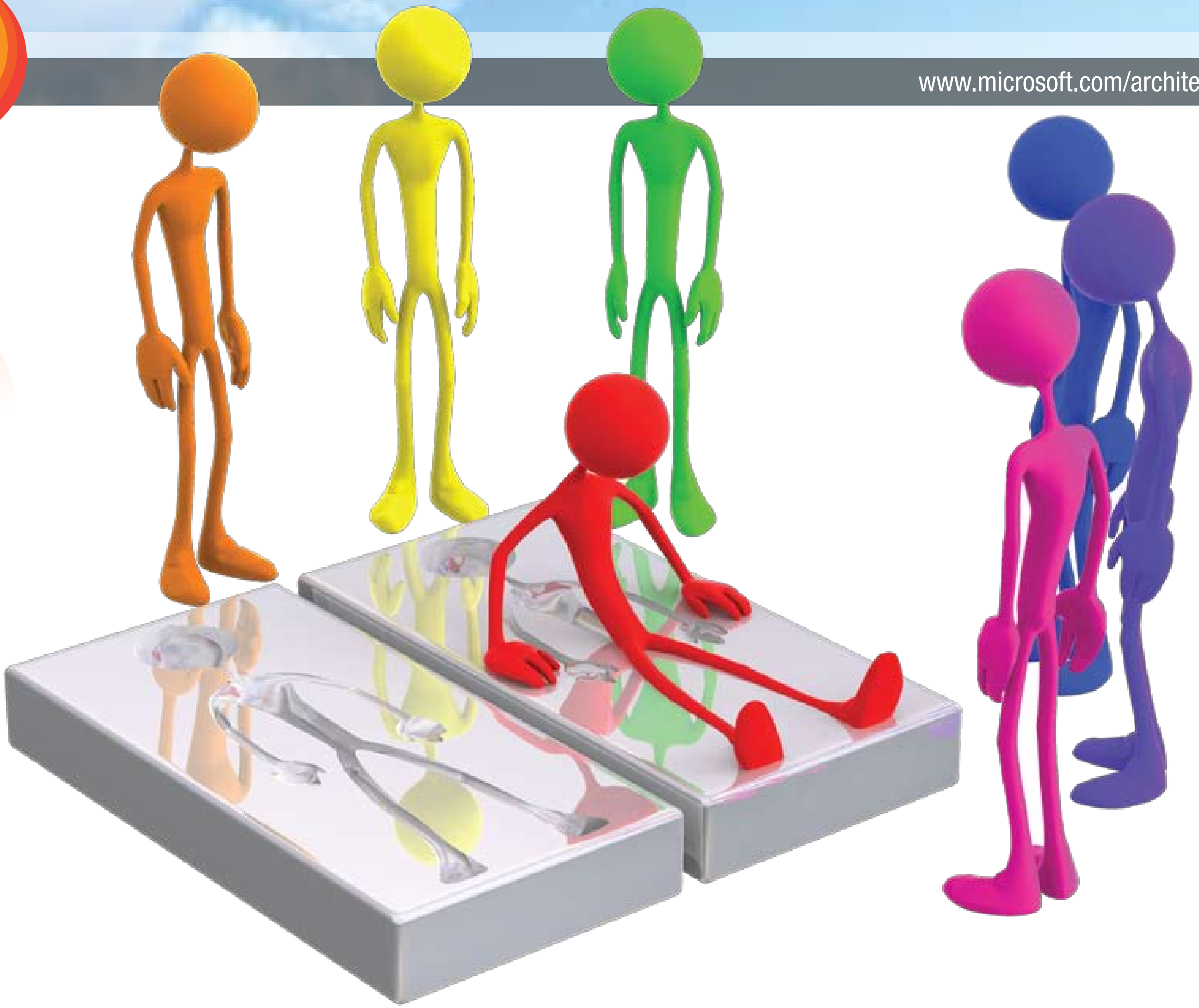
To some, this may make it sound that if you want your internal applications to play in an integrated way by using the 'Geneva' framework, you'd have to insist that your business partners use WS-* protocols and not the SAML protocol.

"It seems that way on the surface," laments Wittenberg. "Typically when organisations federate their identities they do so from organisation to organisation and not organisation to single-application."

This, he says, means they use the 'Geneva' server at the edge of their network to service their application estate.

"The edge server would use any of the protocols to connect to the Internet and would use only WS-Trust and WS-Federation to connect inside the organisation," he adds.

As Wittenberg points out, it's in all the vendors' interests to build identity systems that are interoperable so that when people



buy products from IBM or Novell they will implement those standards in the same way Microsoft does and be able to federate with the cloud.

"The whole point of federation is to link organisations together and there's no guarantee of what infrastructure a business partner has when you strike that deal," he adds. "We all get together at major identity conferences such as RSA and Digital Identity World to run 'interopathons'."

Wittenberg believes that these provide a great chance to not only prove that the products work together, but to also identify bugs that need to be fixed and allow each vendor to produce configuration guidance on how to set a system up when interoperating with a different vendor's product.

"We have a number of guidance documents on Microsoft.com to help with this," he says. "It's important because an IT professional with experience of say Windows, can communicate with the equivalent IBM skilled guy in the other company in a more meaningful way."

In the area of identity, we've seen what Wittenberg refers to as 'a gradual consolidation of standards' as he believes the debate on these is now largely over.

The examples above are the ones that are being adopted and being built into vendor products and frameworks, he says.

"SAML 2.0 represents the convergence of the OASIS specs, much of the Shibboleth system, and the Liberty Alliance ID-FF specifications," he adds. "So the days when you were either Liberty or Shibboleth or SAML are largely over.

Wittenberg suggests the example of a user who logs in to the network at 9am unknowingly using the Kerberos standard.

"They log in to Exchange email, Sharepoint and a few other applications inside the firewall all using Kerberos," he says. "Later in the afternoon they click an icon on the desktop that opens a web browser session to a partner's application. They might use SAML to get to the partner's federation server, Kerberos internally to authenticate their access to that server and WS-Federation to access the application itself. These products are able to do protocol transitions from one protocol to another."

"When you think that you may have business partnerships with other organisations, employees and your end-customers, sat at home on the internet all being able to use exactly the same application, you see how powerful the combination of the cloud and standards can be."

Principles of Privacy

Privacy

Sound architectural principles and identity technologies that ensure privacy need to be agreed upon for successful transfer of data within the cloud. The Arc reports.

You can think of the laws of identity as a set of architectural principles that any identity system needs to observe if it's going to be successful. When we look at systems that have failed to gain popular traction in the past, they've usually ignored one or more of these.

These 'laws of identity' were driven forward by Kim Cameron, chief architect of Identity, Corporate Identity and Access Strategy Team at Microsoft, with the help of friends and peers across the industry. Today, they represent a solid foundation for how the company and competitors alike should develop solutions in this space. Cameron believed that people using computers should be in control of giving out information about themselves, just as they are in the physical world. This means delivering the minimum information solely to those who need it, with details being retained no longer than necessary.

At the same time, he felt it should not be possible to automatically link everything we do in all aspects of how we use the Internet, as a single identifier that stitches everything up would have many unintended consequences. What was needed was a choice in providers for different contexts of identity information. He reasoned that systems should also be built so we can understand how they work, make rational decisions and protect ourselves. At the same time it was noted that devices through which we employ identity should offer people the same kind of identity controls – just as carmakers offer similar controls so we can all drive safely.

"The Identity Metasystem embodies these laws," says Steve Plank, UK identity architect at Microsoft. "What really happened was these principles came along and guided the way Microsoft developed its identity products. By making sure the products adhere to key architectural principles that are being adopted across the industry we build a bigger 'ecosystem' that many organisations can participate in."

As we move towards an era of software plus services concerns for the privacy of information stored in the cloud rumble on. Yet, as Dr Stefan Brands, principle architect, Corporate Identity and Access Strategy Team, Microsoft, points out, the simplest, yet least practical answer is to encrypt data before it is sent.

"As long as you never give the keys to the cloud operators, the data is safe," he says. "But of course you are much more likely to want to to serve up unencrypted data from within the cloud so you need to be more creative."

Although simply allowing the cloud to encrypt the data reduces the attack surface, it doesn't remove it completely. Enterprises could put digital authenticity marks on any data passed to the cloud, which at least preserves data integrity. A third approach, according to Brands, is to spread the data among two or more cloud providers and chop it up in such a way that both parts are needed to calculate the resulting data.

"Compromising one cloud provider renders the data useless to anybody with only one half of the data," he adds. "As the data is recombined at the client computer, no single operator has access to all the data. You can see why being able to accurately identify a bone-fide user is important to security."

Certainly privacy of data is something that must be carefully considered and Brands suggests that with careful architecture of identity elements systems can be built operating in the notion of 'minimal disclosure for a defined use'. "That is," he says, "where a site is asking for your date of birth before it sells you some alcohol. They don't actually need to know your date of birth. All they need to know is that you are over eighteen. So you could build your cloud system to calculate whether that statement is true or false and only pass that on to the consuming service."

Brand also warns against using common identifiers at more than one site, as these reveal aspects of your identity, which when colluded enable sites to get a better picture of who you are. For example telling one site your email address and date of birth whilst giving another your email address and your postcode means your email address is a linkable element.

"Spread that across many tens of sites you might use on the Internet and you have a time-bomb of privacy issues building up steam," says Brands. Identity technology which prevents linkability is key and this is one of the reasons Microsoft acquired Brands' company Credentica.

"Of course the technology can't prevent linkability if you expressly identify something unique about yourself like your name and address or your email address," adds Brands. "But you don't need to use these kinds of identifiers if you combine the technology I developed at Credentica, U-Prove, with say, information cards. That's something we're working on at Microsoft."

Normally when a service holds your data it has to know which site you will use it at so the data can be sent direct to the other party or, if it is to go via the

and the laws of identity

user, be encrypted in such a way that only the other party can read it. This means knowing which partner you are sending data to – even knowing its destination represents a loss of privacy in this sense. "Information cards support an architecture that allows you to send the information via you, to an end service without the claims provider knowing who that service is," explains Brands.

One of the things a relying party wants to know is that the identity data it received genuinely came from a particular trusted claims provider, something which involves applying digital authenticity marks. Normally, says Brands, you'd have to tell the claims provider what information you wanted to 'blind' and only then would they apply their authenticity signature. They'd learn what data you wanted to send to the relying party," he adds. "That could be a privacy issue, so the cryptography I invented allows you to 'blind' data you choose after the claims provider has put its authenticity mark on the data.

Another important aspect within all this is that the legal and policy framework around federated identity is often more complicated than the technology itself. "If you think about the way federated services are set up from a technical perspective," says Craig Wittenberg, lead architect, Corporate Identity and Access Strategy team, Microsoft US. "You install some software, share some keys to establish trust, decide on a common vocabulary of what you'll exchange across the federation relationship, agree how you'll transform the claims you get from the partner and so on."

Wittenberg says this is all encapsulated into software, coded into queries and transformations and so on.

"Well, when you think about legal and policy frameworks they are very similar. You create a standard template which encapsulates how your organisation does business, you then set up a common understanding between the organisations, negotiate remedies that are to be applied if one or the other side breaks the agreement, agree on terms and conditions of the exchanges and so on. It's a very similar idea," he says.

According to Wittenberg, the broad legal and policy elements are common to many organisations in the same way that software requirements are so common that most companies buy commercial off the shelf (COTS) products rather than build their own.

"Of course there is usually some customisation of a COTS product and the legal frameworks we're developing allows for customisation in just the same way," he adds. "It's just a way to give a customer a 'leg-up' because we've found it's rarely technology that slows the adoption down – it's the legal and policy framework. Every organisation has to start from scratch. We're looking at solving that problem."

JARGON...?

COTS:
Commercial Off The Shelf. Software or hardware products that are ready-made and available for sale to the general public. Microsoft Office is just one of these.

Back to the future

The Future

Dr Stefan Brands, principle architect, Corporate Identity and Access Strategy Team and Microsoft's U-Prove inventor, talks to The Arc about the outlook for privacy when applied to software plus services.

Imagine if you will that you wish to allow a user to manipulate data they have been given by a cloud service and yet still maintain the cloud's authenticity signature intact.

The cloud, for example, might send you a complete set of claims and you decide against letting the consuming site know your date-of-birth. Well, with the latest in advanced cryptography you can hide that information in the same way you'd take a thick black pen and scribble over the top of data in a legal document.

"The seal of the legal firm may still be on the document, so you know it came from them, but there are some things in there you just don't need to know, explains Brands. "Or you can derive data, like making the claim that you are over eighteen rather than sending your actual date-of-birth. It's amazing how easy it is to identify an individual with a very minimal set of data."

Brands suggests thinking about the road where you live. If you have a date-of-birth and a postcode there is a very high chance you are the only person in that postcode with that date-of-birth.

"Turn that claim in to 'over18=true' and the problem becomes much more difficult to an identity fraudster," he says.

Although this technology has yet to be incorporated into any of its products, this is an area Brands says he and Microsoft have been exploring with the development of its U-Prove product line which it claims also solves the problem of websites colluding to gain a bigger picture about you.

Another area in which the company has been working is anonymous accountability – one that causes a fair amount of head scratching for most.

"The default belief most of us have is that we need to know who you are to hold you accountable for something," explains Brands. "However, we've developed privacy techniques using cryptography and piggy-backing it on to the Identity Metasystem model in a way that protects the privacy of the user."

This means that if services are abused in some way users can still be denied access without the service provider knowing exactly who they are.

This type of technology will become more important as cloud computing services start to interact with each other through users. Users will have multiple relationships with software running in the cloud, but they'll want to maintain their privacy from one operator to the next. This will more than likely mean that those cloud operators who offer services respecting privacy will be the most successful.

Yet the operators of these services still want to control the behaviour of their end-user customers in such a way that they don't cause disruption or other damage to the service or other consumers.

"Doing this in a way which preserves anonymity but denies a service or feature is therefore going to be an increasingly important part of the default feature-set of cloud operators," adds Brands.

Microsoft is also doing work in specialised areas of cryptography, like searchable encrypted data, which should prove very useful for those operating in the cloud.

Here, the data is encrypted in such a way that you can search for pre-configured keywords.

"You can see how this would be valuable to some database applications where the query criteria are known in advance," adds Brands. "It means data in the cloud is protected from insider attack as well as the outsider attack. Even if there was a catastrophic failure and information leaked from one customer's part of the cloud to another's – the data would be useless to them."

Another area of importance is 'multi-party security.

"In finance, you might have an auditor who needs to know the average value of a set of financial transactions between a collection of banks," says Brands.

Indeed, it is possible to have a cryptographic protocol that allows you to retrieve that answer without any central authority knowing the individual amounts from each bank that go to make up the average.

"This is obviously important for privacy," he adds. "The auditor needs to be assured the banks are operating within certain financial limits, but the privacy of each bank's data is maintained."

The Identity Metasystem brings several benefits to those companies who want to connect to the cloud. As a universal system for the exchange of identity information, it means any organisation can plug their cloud and their enterprise resources into it in rather the way we plug USB adapters in to our laptops. They are all designed to fit and work together even if their identity infrastructure is from a competitor's products.

Of course, there are many concerns as to the privacy of information stored in the cloud and enterprises must consider how they protect against this.

Those who are clever will be looking into encrypting data prior to sending, withholding keys from operators, adding digital authenticity marks to data passed through the cloud, and chopping this between operators as they look to shore up their fences and defend their assets. Spreading the load and responsibility certainly also makes sense, in the same

way that clever architecture lends itself to systems operating under the notion of ‘minimal disclosure as previously discussed in this issue.

When you build a service, or indeed when you use the identity service of another provider, Brands says applications can use privacy enhancing technologies like information cards.

Normally when one service makes some claims about you and passes that data onto the consuming service, you have no way of interacting with it, inspecting and seeing if you are happy about what’s going to be revealed about you, before bailing out of the transaction entirely should you wish. Instead, this all just happens under the covers and you are left with having to trust policy statements.

With information cards, user-centric identity is used. This means a data structure called a security token is sent to you containing a digital authenticity mark to say it was genuinely issued from the specified service. You can then use the Information Card software on your computer to ask yourself questions such as why, when putting in for a newspaper subscription, a company might want to know your date of birth?

The software has choices for ‘optional data’ – so the company requesting this makes it clear to you they will still process your transaction, but you can opt out of sending the optional data.

This differs to traditional techniques used as the data is delivered to your computer and it’s up to the user to click the ‘send’ button.

“You are put in total control of your identity data,” adds Brands. “It’s not like you click a button on a website and you’re never sure how the data, or even what it was, got to the endpoint.”

theARC magazine

www.microsoft.com/architect