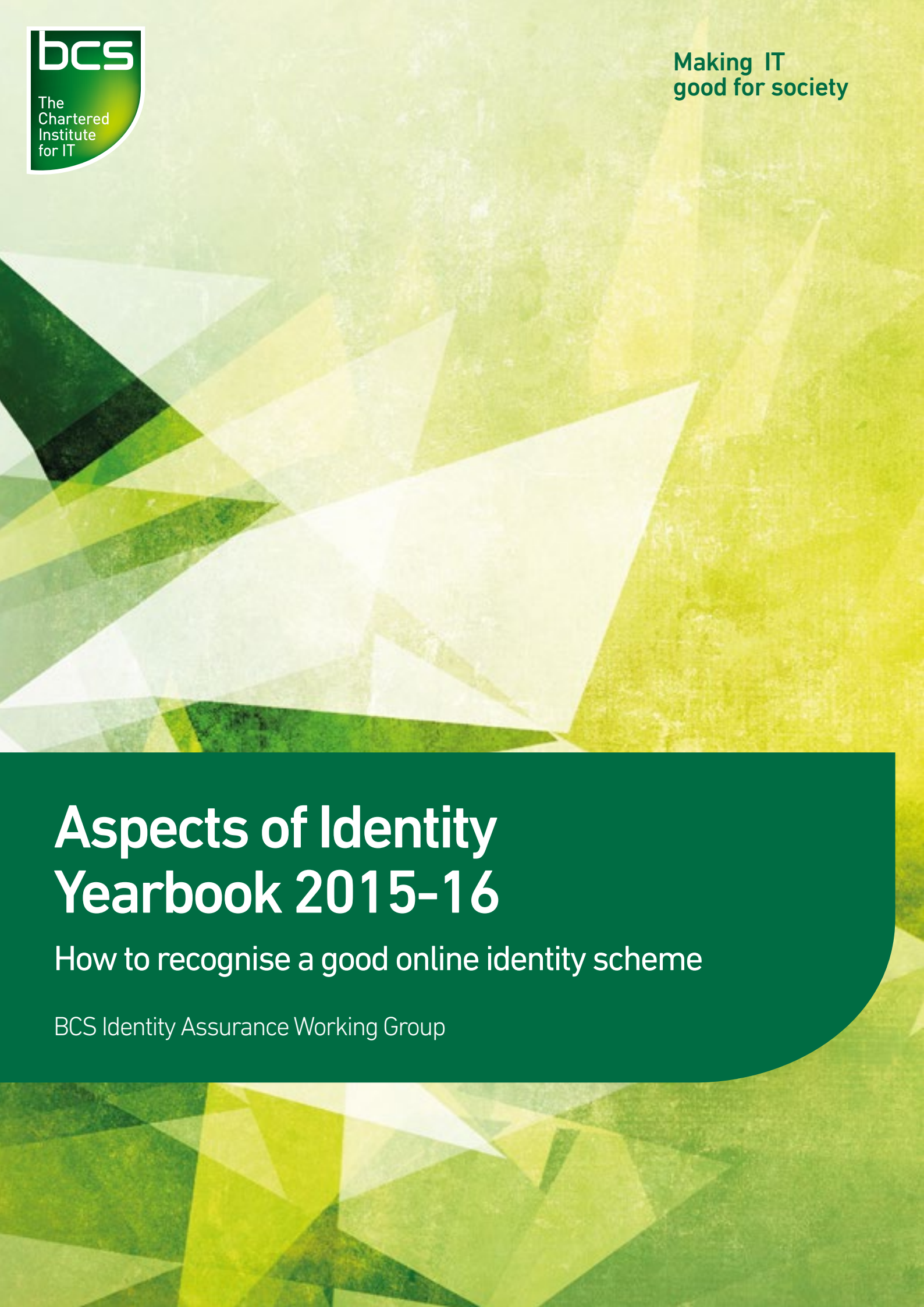

Aspects of Identity Yearbook 2015-16

How to recognise a good online identity scheme

BCS Identity Assurance Working Group

How to recognise a good online identity scheme

Over the last five years the Identity Assurance Working Group (IAWG) has been examining governance and other issues surrounding identity assurance on the internet. Readers can find the annual yearbooks and follow the development of thinking around the topic at **policy.bcs.org/content/identity-assurance-working-group**

'On the internet, nobody knows you're a dog!'

Our 2015/16 Yearbook takes a different form from its predecessors. We consider how we might recognise a good online identity scheme. The need for online identity assurance is seemingly outstripping the availability of schemes capable of countering the ever increasing levels of online crime. Identity assurance is one of several measures that national and international law enforcement urgently needs. Shielding the benefits of the internet from its inherent vulnerabilities is proving an exceptionally difficult challenge. A wide range of crime, including theft, child exploitation and people trafficking, is made easier by the lack of robust, provable online identity. Anonymity also breeds antisocial behaviours such as trolling and online bullying. We are some way off from having identity assurance schemes that can instil a sense of confidence and reassurance in the online population.

So what distinguishes a good online identity scheme from a poor one? How will we judge objectively any emerging scheme? Perhaps the essentials of a universal scheme already exist? Here we take a look at the many aspects involved in answering those questions for any online identity assurance scheme. For some of the aspects we highlight, there are potentially 'good' and 'bad' answers; however, for many others there are merely choices to be made. Also, because it is probable that a successful large scheme will have started as a successful small scheme, we should not expect any emerging candidate scheme to tick all the boxes from the start.

The purpose of a scheme - What's it for?

We start with the most basic question. What activities (use cases) does the scheme aim to support? The basics add up to a daunting list. Does it facilitate financial transactions (buying, selling, managing finances)? What about claiming benefits and subsidies? Paying tax? Does it support personal record-keeping such as health and fitness? Activity location and tracking? Age verification? Criminal record status? Power of Attorney? Does it offer safety and protection to legal pornography and gambling? The internet facilitates all of these, so perhaps a universal identity assurance scheme, maybe in the form of several compatible schemes, needs to do so too.

Levels of assurance – How strong is it?

Any online identity scheme has to deal with the fundamental problem of identifying someone with a useable level of assurance when they are remote from you, over an untrusted network and in an unsupervised environment. The level of assurance required is key. It is useful to have different levels of assurance to handle different business requirements. This can keep the cost and complexity down when just providing information or basic services, but it also allows for strong levels of assurance when fraud and identity theft may be a real issue.

Once an identity is established within a relationship does it need to be re-usable? If yes, we must ask how this is to be achieved. Are the credentials associated with the identity as strong as they need to be for the transaction?

The final aspect is that there is no trust in the Internet. Therefore, can the connection be encrypted if strong levels of assurance are required?

Target market – Who's it for?

Is the candidate scheme rooted in the private sector or the public sector? Does it serve both effectively?

Which types of service provider does it serve? Does it prove my identity (or aspects of my identity) to service providers throughout the UK? Does it work internationally (i.e. in other jurisdictions) for any service providers anywhere? Can more service providers join easily? Wherever it works, which users does it serve? Does it prove the identities of the settled population? Of visitors too? Of anyone anywhere?

Is the service legal in some jurisdictions and illegal in others? How does it avoid entrapping users in countries where it is not legal? Can oppressive states block it, subvert it or harass its users?

How do users know they're dealing with the real online identity scheme and not a spoof? Does it provide mutual verification (i.e. the user to the service provider and the service provider to the user)? Mutual verification of identity is most important for personal or financial information such as credit card details.

Do the scheme enrolment mechanism and credentials support the whole target audience, whatever ethnicity, languages and disabilities that may involve?

How to recognise a good online identity scheme

Commercials – Who pays?

He who pays the piper calls the tune. In this case there are set up costs and running costs. Who is paying to set up the scheme? Who pays for each transaction? If they don't pay, what fails and who chases the debt? How are the parties incentivised to resolve payment disputes, conclude the transactions and keep the scheme going? Will subsequent transactions continue when someone hasn't paid, or does their service reduce or cease?

Who does the money go to? Is any party inherently privileged or locked in? Is that a commercial organisation? Who ultimately pulls the strings? Do I have to accept advertising if I want to use the scheme?

Liability – Who carries the can?

Who is liable for each transaction? Is liability dependent on the circumstances? Liability is an inherent aspect of trust. High-assurance transactions over the world's electronic networks recognise few conventional borders or sectors, so the transacting parties cannot rely on Governments to pick up the tab when things go wrong.

What happens if liability is disputed or can't be proven? Who ultimately underwrites the scheme? Any candidate scheme needs to show how liability is always clear, whatever the circumstances.

Who cares for the scheme to protect it from collapse?

Practicalities and ease of use – How well does it work?

Does the scheme work equally well for everyone, all ages and all lifestyles? Does it work better for some sections of society than for others? Is there a minimum age?

Can I remain anonymous while the scheme proves my credentials, or am I always identified to the other party? Does the scheme put me at risk of persecution for my beliefs or lifestyle? Can I leave the scheme?

How easy is it to use? If I only use it occasionally is it just as easy? Is it fast? Does it work on all devices? If a transaction fails, how do I find out why?

Is the effort involved proportionate to the risk?

These questions on practicality and ease-of-use assess whether the scheme supports equality across the target audience, regardless of their status or ability in the digital or physical worlds. How does the scheme ensure that this is always so? How can the scheme's users see for themselves that they are all treated equally?

Is the scheme locked into specific technologies or can it evolve? Can it keep up with changing usage patterns?

Moves and changes – Can I easily update my credentials?

Can I change my name and address? My email? Can I make changes as often as I like? Does each change affect (degrade or improve) the strength of the scheme? Can I change my gender? Does the scheme support the formal gender-change processes?

Can I have multiple names (aliases)? Are they linked or independent of each other?

Record-keeping – Where's my digital exhaust?

Does the scheme keep lasting records of usage (an audit trail)? Does it create records for others to keep? Who can access those records?

Does it support my right, in applicable jurisdictions, to be forgotten or de-indexed? Even in cases where a user ceases using a particular online identity scheme, and asks to be 'forgotten', some records may need to be left in place for specific targeted fraud, security or other criminal investigation purposes.

Can I access, and see who can access, my data? Can I find out who has rights of unaudited access to my data?

Online identity schemes should process only the minimum data needed to fulfil a user's request in a secure and auditable manner. However, records need to be kept both for practical and legal purposes. An online purchase, for example, may need to be delivered to an address and the supplier may need to keep records to honour any warranty, perhaps over several years. Records need to be kept for accounting and legal purposes, including in case the transaction is referred to an ombudsman or is the subject of court proceedings.

Interoperability – Does it share my identity?

Does the scheme recognise the existence of other identity schemes? Are those identity schemes online or not?

Does the candidate scheme trust other identity schemes? Does it assist other identity schemes? What are the consequences for the candidate scheme of interacting with other identity schemes in these ways? What about its use of other specialist services that support identity schemes, such as credit reference agencies and banks?

In an increasingly interconnected space, questions arise over the extent to which users have control of their identity or identities. If an online identity scheme is capable of sharing identities with another identity scheme, can the individual control whether and how that is done?

How to recognise a good online identity scheme

Cyber – Is it at risk?

How well protected is the scheme from cyber risks? What kinds of vulnerability does it have? Denial of service? Loss of transaction integrity? Theft of credentials? Failure to keep records? Impersonation? Phishing?

Under attack, does it degrade gracefully or catastrophically?

Who is protecting the scheme from cyber-attack? What world-class resources can they call on to do it right?

Identity schemes are no less liable to cyber-attack than other online services, perhaps more so given their role. Over a scheme's lifetime it will be attacked and there's a good chance it could be compromised somehow, perhaps more than once. Does the scheme design cater for effective incident management? Are the implementation of the scheme and the procedures for operating it robust and resilient?

Scheme creators face choices on how open the scheme should be and whether they should place their scheme under Government protection (if that option is available). Does the scheme have national or international protection? Does it rely on open source practices of public scrutiny? How can the user know that the scheme is adequately secure? If there's a kitemark showing audited compliance with a set of standards, whose standards are those, how often should compliance be confirmed and how promptly should any weaknesses found be corrected? How can individual users resolve their problems and their concerns?

Fraud and error – Who's checking?

Is there a counter fraud operation? Is it proactive or reactive? Is it effective evenly across the user population?

How does the applicable jurisdiction relate to the location of the transaction activity? What offences can the parties be judged to have committed? How will prosecutions follow? Who decides whether to prosecute? This is a serious issue with trans-border interactions. A website may appear to be in the UK but actually be elsewhere. By setting up an account you agree to their terms and conditions. If something goes wrong it may be very difficult to seek redress if the website is operated under another jurisdiction.

Who is countering entropy and keeping the scheme accurate? Who is correcting errors? Who decides what is an error and what is not? How easy is it for someone else to steal or misuse my identity, or to register as me?

There are a wide variety of issues that need to be thought about and addressed in any identity scheme, in order to counter fraud and error. Fraud is the fastest growing issue because everything that can be done online is being done online and so the money and also the personal information that has real value is moving there.

Restitution and redress – Who handles disputes?

How does the scheme resolve disputes? In all transactions, whether physical or online, the parties typically pre agree their respective responsibilities for all foreseeable circumstances. In practice these agreements evolve over time to correct ambiguities and errors and to include previously unforeseen situations. The effort expended on this is usually in proportion to the level of assurance provided and the inherent value of the types of transaction that are involved. It is generally much more difficult to reach an agreement after something has gone wrong than beforehand, so good schemes will always put the necessary effort in up front.

Building confidence, recognising innovation

All candidate identity schemes will have their particular strengths and weaknesses. In the short term, some might legitimately pick off particular use cases, such as age verification or payment, or sections of society (perhaps those with bank accounts or passports or a permanent address). Ultimately, though, the whole spectrum of use cases needs to be supported by one scheme, or perhaps by several interoperable schemes, so that all needs are met coherently. That challenge may take years to fulfil, but we are confident that it will eventually be met.

Meanwhile the important thing is not whether any candidate scheme answers each question in a particular way, although some questions are inherently judgemental. Rather, it's about the credibility of a candidate scheme's answers to all the questions, taken as a whole. For a scheme to be credible it needs to be able to tell a good and consistent story in all these dimensions, so that it delivers a trustworthy and convenient service within whatever scope it chooses to address. At least until innovation produces something better.

At BCS we will continue to look at all innovations in identity assurance as critical friends. We don't have a favourite solution. But we are conscious of the scale of the challenge facing the online industry to redress the balance and make the Internet a safe and secure place for all of its users, whoever and wherever they may be.

If you would like to have an electronic version of this document and pass it on to others it can be found at **policy.bcs.org/content/identity-assurance-working-group**