Forensically ready digital identity management systems, issues of digital identity life cycle and context of usage

Mehrdad Tajbakhsh

Accounting and Management Faculty,
IT Management Department,
Shahid Beheshti University, Iran
Email: me.tajbakhsh@webmail.sbu.ac.ir

Elaheh Homayounvala*

Cyberspace Research Institute,
Shahid Beheshti University, Iran
Email: e_vala@sbu.ac.ir
*Corresponding author

Sajjad Shokouhyar

Accounting and Management Faculty,
IT Management Department,
Shahid Beheshti University, Iran
Email: shokohyar@sbu.ac.ir

Abstract: Collecting necessary digital and network forensics to prove the identity of an individual who is responsible for a crime, or suspected of a malicious attack, or has used a device during an incident, with minimum doubt to the court or other legitimate organisations based on the digital forensic investigation model is one of the most important legal and security issues of digital identity management systems (DIMSs). Without a good understanding and identification of the most important parameters of DIMS based on the digital forensic investigation model, it is not possible to do digital forensic investigation and provide required evidence. Therefore, the main goal of this paper is to identify and prioritise DIMS parameters by considering a user's digital identity lifecycle, the contexts of usage challenges, and constraints that should be considered in a digital forensic readiness model.

Keywords: digital identity; digital identity management systems; DIMSs; digital forensic investigation process; forensic readiness.

Reference to this paper should be made as follows: Tajbakhsh, M., Homayounvala, E. and Shokouhyar, S. (xxxx) 'Forensically ready digital identity management systems, issues of digital identity life cycle and context of usage', *Int. J. Electronic Security and Digital Forensics*, Vol. X, No. Y, pp.000–000.

Biographical notes: Mehrdad Tajbakhsh has served the last 15 years as an Official Expert IT and ICT Engineer to the I.R. IRAN Judiciary Court. He received his MSc in Information Technology – Advanced Information Systems from Shahid Beheshti University (SBU) in Iran. Current article is extracted from his Master degree thesis at SBU. He received his Bachelor degree in Computer Engineering from Tehran University (TU), Iran in 1992. Currently, he is doing research on his second Master degree in Information Technology – Information Security at Tarbiat Modares University (TMU), Iran. His research interests are digital identity, digital and network forensics evaluation and accountability parameters, Intellectual properties evaluation and cost analysis.

Elaheh Homayounvala received her PhD from King's College London in 2006. She is an Assistant Professor at Cyberspace Research Institute, Shahid Beheshti University (SBU) in Iran. Before joining SBU, she was a research associate at King's College London, University of London, UK and Iranian Research Institute for Information Science and Technology. She received her MSc and BSc from Sharif University of Technology in Iran. Her research is multi-disciplinary and includes information and communications (ICT) management, digital identity management, user modelling and personalisation.

Sajjad Shokouhyar has been an Assistant Professor at the Department of Management and Accounting in Shahid Beheshti University (SBU) in Iran since January 2014. He received his PhD in Industrial Engineering from Polytechnic of Tehran in Iran. He received his MSc and BSc in Industrial Engineering from Amirkabir University of Technology (AUT) in Iran. His research interests include data mining, soft computing, supply chain management and organizational issues.

1 Introduction

The introduction of new IT and ICT technologies has helped online services and facilitated greater information sharing through the internet. This new cheaper and faster access has resulted in users' access to online transactions and a wide range of online services. This new environment of communication comprising sharing information and business has created challenges and caused concerns about security and the legal aspects of digital environment. Identity information of people using the internet and sharing information, either intentionally or inadvertently, can be used by others or stolen by other parties. The advent of social networking sites, along with the near-ubiquitous availability and use of the World Wide Web has significantly changed the ways in which users communicate and share information (Jones and Martin, 2010). The increasing number of criminal reports and warnings about cybercrimes due to the illegal use of user identity and stolen information clearly explains the importance of security and privacy challenges for social networking sites and different internet applications (Perez, 2009; BBC News, 22 July 2007).

At the same time, new technologies support the increasing demand for access to information at any time or place. As a result, while determining the identity of a user on a network or a device is not so easy, the range of devices that must be examined and the storage capacity of these devices have continued to increase. Technological advancements have not only made it increasingly easy to gain access to information, but

they have also made the issue of identifying the user more difficult as the credentials that they have to use to 'prove' their identity have had to become more international, more electronically based, and as a result, more difficult to validate. Embedded chips that store digital identity information to protect digital information and make it harder to forge documents may be used in e-passport and e-voting (Jones and Martin, 2010). According to Mueller et al. (2006) the context of usage is an important parameter for users to select their identity type and its attributes. Therefore, the type of digital identity management systems (DIMS) and their characteristics to manage a user's digital identity (DI) lifecycle are strongly related to the context of usage, applications and online services.

1.1 Digital identity

An entity should be described as a set of characteristics and attributes forming a domain-based identity. There are differences between the defined identity of an entity in a social network and that on e-commerce applications. Most popular examples of identifiers are as follows: username/password, individual biometric information, digital signature and certificates, which are used in specific domains or contexts (Wayman, 2008). Hence, DI is defined as *the identity resulting from the digital codification of characteristics and attributes in a way that is suitable for processing by computer systems* (El Maliki and Seigneur, 2007) *digital identity refers to the aspect of digital technology that is concerned with the mediation of people's experience of their own identity and the identity of other people and things* (Cameron, 2005). National identification number and passport number, which are social identifiers, biometric information such as fingerprints and other information including email address, date of birth, etc. constitute identifiable information for an individual.

The process to uniquely identify individuals according to their attributes and characteristics as entities in a specific context is called identity management (Leskinen, 2012).

1.2 Digital identity management systems

Identity management through computer networks is commonly described as *the combination of technologies and practices for representing and recognising entities as digital identities* (El Maliki and Seigneur, 2007). DIMS is defined as *identity management (IdM) is the framework used in computer or communication systems to control identity* (Dabrowski and Pacyna, 2008) or DIMS is *the resource access control and identity information management implemented with new technology, the goal of IdM is to cut off the cost to manage users and their identities, attributes and access privilege to improve productivity and security* (Cao and Yang, 2010).

Every DIMS consists of components that can be called a *user*, who wants to have access to a service, identity provider (IdP), which is the issuer of user identity. Service provider (SP) is the relay party imposing identity check, which is a set of attributes of the user (Banihashemi et al., 2016; Spantzel et al., 2006).

In the past users usually had one identity, but in current internet usages and online services it is acceptable for a user to have more than one DI for different online interactions. Due to the user's entitlement change over time, it is necessary to change its permission and access control of her/his identities and handle them in a centralised way

(Windley, 2005; El Maliki and Seigneur, 2007). This is known as DI lifecycle which comprises four steps:

1 enrolment

2 management

3 support

4 deletion at the end of the lifecycle (Table 1)
(Windley, 2005; Hansen and Meints, 2006).

Within an organisation DI lifecycle is a three-step process involving initial identity set-up, identity maintenance and identity termination (Mueller et al., 2006).

Table 1 Steps of the identity lifecycle

- Enrolment – creation of accounts for new employees:

  Initial issuance of the credentials and setting of the access permissions needed by the new employee.

- Management – maintenance of accounts:

  In a changing working environment (promotions, changes of departments) the 'user and access management' needs to handle the changing access permissions for the enrolled users (in order to minimise liabilities).

- Support – changing of authorisations:

  Issuance and re-issuance of credentials (e.g. reset password).

- Deletion – end of lifecycle:

  Revoke or freeze user-accounts or entitlements.

Source: Based on Windley (2005), Hansen and Meints (2006) and Mezler-Andelberg (2008)

Every DIMS should be elaborated to deal with the following core aspects (ICPP and SNG, 2003; Banihashemi et al., 2016):

- *Management:* the number of digital identities per person will increase, so users need convenient support to manage these identities and the corresponding authentication. Managing digital identities does not only mean handling new and fixed identities within one scope, but also handling the complex situations of changing identities in changing scopes, and managing the different perceptions of identity within the same scope (Alpár et al., 2011).

- *Reachability:* the management of reachability allows users to handle their contacts in order to prevent misuse of their address (spam) or unsolicited phone calls. By using DIMS, one implicitly agrees to several complex and poorly understood trust relationships between the parties that belong to that identity management system. The user trusts the IdP not to act on its behalf without his/her explicit consent. In many systems for identity management, the IdP essentially does the logging in to the SP, on behalf of a user. It can easily do so, without the user even being present. Clearly, the user does not want the IdP to do this. Additionally, the user expects the IdP not to release personal information unless explicitly asked by the SP and with the

permission of the user The relying party trusts the IdP not to extend the circle of trust (without his/her consent) (Alpár et al., 2011).

- *Authenticity:* ensuring authenticity with authentication, integrity and non-repudiation mechanisms can prevent identity theft. To prevent phishing attacks it is very important that users are able to authenticate the SP and the IdP. Mutual authentication, therefore, needs to be incorporated in identity management systems, in such a way that the user is not required to install special software or to use one and the same computer all the time (Alpár et al., 2011).
- *Anonymity and pseudonymity:* providing anonymity prevents tracking or identifying the users of a service. To enhance user privacy, it is recommended that users can remain anonymous or use pseudonyms at SPs, and to have IdPs that do not link all user transactions at all SPs together. Although identity management systems already implement some of these solutions, not all of these have been put to use. Identity management system are required not to allow IdPs to see all user transactions, without violating the law of location independence (which states that identity management systems should not rely on any persistent data stored locally on the user's machine) (Alpár et al., 2011).
- *Organisation of personal data management:* a quick method to create, modify or delete work accounts has considerable significance, especially in big organisations. Identity management systems should provide a way to automatically determine the full set of required credentials for a certain service and the minimal role the user can assume that covers those credentials, and they should also put the user back into control and support the user in maintaining a user profile that can be used (in a controlled manner) by businesses in several organisational domains (Alpár et al., 2011).

1.3 DIMS digital forensics

Digital forensics deals with the investigation of computers and other digital devices that are believed to have been used in criminal activities (Francia and Clinton, 2005). DIMS digital forensics involves the application of methodologies and tools to capture and analyse DI transactions in DIMS that can be presented as evidence in a court of law (Jones and Martin, 2010). "A digital forensic process is a procedure that is followed to investigate a particular criminal activity involving digital evidence" (Casey, 2001). Digital forensic investigation (DFI) is a three-step process involving the following: *acquiring the evidence* while ensuring that integrity is preserved; *authenticating the validity of the extracted data*, which involves ensuring that it is as valid as the original; *and analysing the data* while keeping its integrity.

The security properties of DIMS the capabilities and characteristics that are helpful for protecting and collecting digital evidence for personally identifiable information by considering its related DFI challenges are critical factor to the success of an identity management service. Therefore, one of the most important evaluation factors of DIMS is its capabilities for DFI, facilitating collection and storage of DIs and transactions in DI lifecycle as digital evidence, which prevents violation of a DIMS's core features and minimises its side effects.

Providing proper evidence in order to prove who is responsible for a crime is one of the challenges for DIMSs today. Therefore, a DIMS should provide an easy way to the internal or external auditor for assessing the security and DFI capabilities and for collecting DF by considering digital identity lifecycle and contexts of usage challenges in digital forensic investigation model (DFIM).

So any evaluation of DI parameters as DF in the DFI process should be done by considering DI lifecycle and the context of usage or type of online services.

Computer fraud and crime are growing day by day, but unfortunately less than two percent of reported cases result in confidence. DFI emerged in response to the escalation of crimes committed using computer systems and digital environment (i.e. the internet and online services) either as an object of crime, an instrument used to commit a crime or a repository of evidence related to a crime (Agarwal et al., 2011). A DFI is the process to determine and relate extracted information and digital evidence to establish factual information for judicial review (Ieong, 2006). Ieong (2006) and Köhn et al. (2008) emphasise the need to establish factual information as the outcome of such investigation. As discussed earlier in this paper, one of the most important challenges for DFI is to find the actual perpetrator of a crime or fraud in digital environment (Agarwal et al., 2011). Thus, to successfully find DI information related to the actual perpetrator of a crime, using DIMS, which has developed with proper capabilities by considering DFI requirements, regulations and priorities, is a necessity. Identifying and prioritising DI lifecycle parameters by considering contexts of usage of DIMS will help us to develop a DFI-ready DIMS.

DFIM attempts to address some of the shortcomings of previous methodologies, and provides the following advantages: a consistent, standardised and systematic framework for digital forensic investigation process; a framework that works systematically in a team according to captured evidence; a mechanism for applying the framework according to a country's digital forensic investigation technologies; and a generalised methodology that judicial members can use to relate technology to non-technical observers (Agarwal et al., 2011). There are various process models to describe the steps and processes to follow during digital forensic investigations. During such investigations, it is not only the digital evidence itself that needs to prevail in a court of law; the process followed and terminology used should also be rigorous and generally accepted within the digital forensic community (Kohn et al., 2013). In this article, integrated DFIM (Kohn et al., 2013) is assumed as a DFIM having a four-step model in order to identify and prioritise DI lifecycle parameters by considering contexts of usage for DFIs. The four steps of the model are as follows: the readiness phase (the goal of this phase is to ensure that the operations and infrastructure are able to fully support an investigation), *the deployment phase* (the purpose is to provide a mechanism for an incident to be detected and confirmed), *the physical crime investigation phase* (the goal of this is to collect and analyse the physical evidence and reconstruct the actions that took place during the incident), and *digital crime scene investigation phase* (the goal is to collect and analyse the digital evidence obtained from the physical investigation phase and through any other future means).

1.4 Forensically ready DIMS

The purpose of digital forensic readiness is to reduce the effort involved in performing an investigation while maintaining the level of credibility of the digital evidence being

collected (Ngobeni et al., 2010; Endicott-Popovsky et al., 2007). The decrease in effort includes reductions in the time and the cost of incident response.

Minimising the cost of the DFI process as well as maximising the usefulness of collected DF is the goal of any successful DFI process (Tan, 2001). A digital system that is capable of minimising the cost of collecting digital evidence and maximising the usefulness of collected digital evidence during DFI is called DF ready system. DFI in DIMS that is 'forensically ready' can be done rapidly and efficiently. In general, reducing the time involved in collecting digital evidence reduces the cost of the investigation.

Ngobeni et al. (2010) discuss evidence preservation and time to execute, which are affected by technical and nontechnical factors including the following:

- *How logging is done*, the strength of the evidence collected will improve as findings are 'validated' by multiple data points.
- *What is logged:* what is not logged is lost. Every application on every system or device on your network represents a logging opportunity.
- *Intrusion detection system (IDS):* once the argument was whether host IDS (HIDS) or network IDS (NIDS) was better. Today, as evidenced by the merging of HIDS and NIDS in the market place, a mixed solution is necessary. This is complimentary to the forensics-oriented desire for multi-tiered and centralised logging.
- *Forensic acquisition:* forensic acquisition should follow intrusion detection in a timely manner. As such, much of the forensic readiness effort should be put to deciding how evidence will be acquired from any computer or other device used on the network.
- *Evidence handling:* evidence handling represents the 'rest of the equation' after evidence has been acquired. This includes chain of custody, network transport, physical transport, physical storage, and examination.

As discussed earlier, the importance of the DI lifecycle in DIMSs, along with their context of usage and their important roles in DFI, has led IT specialists to use the following criteria for identifying and prioritising the DI lifecycle and the context of usage parameters to develop DIMS which is most suited for DFI readiness.

- *User-centric identity paradigm:* user-centric approach to identity management is a promising way to improve user experience, and thereby the security of online services (i.e. online banking) as a whole. This has the potential to stimulate increased uptake of online services (El Maliki and Seigneur, 2007; Spantzel et al., 2006). However, selecting the parameters that improve user experience may bring some constraints for using DIMS with capabilities of collecting and storing DI information as DF in DFI. For example, when using DIMS in DFI to collect digital evidence, parameters that provide SP (relying party) and IdP the ability to control user experiences and transactions in DIMS will be helpful to monitor and preserve the conditions for collecting DI information and using them in DFI.

- *User's security and privacy:* since identity information is often private and confidential, it is important that suitable privacy and security techniques be adopted for its protection (Bertino et al., 2009) in the context of usage and type of application. It seems DIMS with more restriction on a user's security and privacy would be helpful for DFI, but usually these parameters put more restrictions on DF collection and moving towards forensically ready DIMS.
- *User's legal perspective:* it deals with user control over his/her identity information and defines the disclosure policies of his/her identity information to other parties (Barisch et al., 2010; Lee et al., 2009). A DIMS that is concerned with user's legal perspective can be suitable and helpful for DFI. Consider the following scenario in case of 'least information disclosure', which means not only the smallest number of claims but also the least likely information to identify a given individual across multiple contexts. For example, if a scenario requires proof of being a certain age, then it is better to acquire and store the age category rather than the date of birth. Date of birth, along with other claims, is more likely to uniquely identify a subject and therefore represents 'more identifying information' that should be avoided if it is not needed (Cameron, 2005). Therefore, as discussed in this scenario, the 'least information disclosure' parameter in DIMS will introduce more constraints in DFI and the confined range and variety of information collected for DI as DFI.
- *Types of DIMS:* depending on the types of DIMS (isolated, centralised, federated or anonymously federated), DI parameters and their evaluation metrics differ (Leskinen, 2012). Federated identity management offers the possibility of providing a familiar and consistent user interface for users with respect to login, account sign-up, and identity management activities on the web (http://www.network-forensic.net/form2/PID02-04). Federated identity management is a set-up where identity is shared across domains (Maler and Reed, 2008). It has security considerations that involve multiple security domains, weak user authentication in the web identity chain, and privacy issues as sharing personally identifiable information is often a key goal. It seems that due to the challenges of the federated identity management architecture, proposing a simplified (not only single) sign-on would be useful to collect and store DI information for DFI.
- *Types of application (context of usage):* social network communities facilitate the sharing of identity information in a directed network. Compared to traditional methods of identity information disclosure, such as a campus directory, the social network community fosters a more subjective and holistic disclosure of identity information (Bonneau et al., 2012). Different SPs require different DIs. Different types of DIMSs are used by different types of online services and computer applications (i.e. the website of a bank). Therefore, using DIMS with preserved capabilities for DFI by considering context of usage and application is an important criterion to evaluate DI lifecycle parameters as DF in forensically ready DIMSs.

In order to succeed, identity management solutions must consider identity rules by considering the above-mentioned criteria along with minimising the cost of DFI process. The aim of this paper is to identify and prioritise DI parameters by considering their role as digital evidence in forensically ready DIMSs.

To identify and prioritised DI lifecycle parameters and DI parameters in the context of usage of a DIMS by considering the DI role as DF in forensically ready DIMS, this paper has used empirical experiences of digital forensic investigators and IT and ICT experts.

Hence, in the first step, this paper tried to propose a list of DI lifecycle parameters in a sample federated DIMS [i.e. a DIMS being used in a hospital information system (IS)] by considering DI role as DF, then prioritised the above-mentioned parameters for DI lifecycle based on AHP evaluation method. In the second step, the paper proposed a list of DI parameters in a DIMS by considering their role as DF in the context of usage and tried to prioritise these parameters based on analytic hierarchical process (AHP) evaluation method.

The AHP is a theory of measurement through pairwise comparisons and relies on the judgements of experts to derive priority scales. These scales measure intangibles in relative terms. The comparisons are made using a scale of absolute judgements that represents, how one element influences another with respect to a given attribute. The judgements may be inconsistent, and how to measure inconsistency and improve the judgements when it is possible to obtain better consistency is a concern of the AHP (http://www.network-forensic.net/form/PID01-09).

This paper is structured as follows. Section 2 presents a literature review. Section 3 discusses the DI lifecycle parameters in DFI and introduces a new set of evaluation and design criteria and the materials used to create these parameters. Section 4 discusses the DIMS parameters to collect DI as DF by considering contexts of usage and introduces a new set of evaluation and design criteria and the materials used to create these parameters. In Section 5 the proposed parameters in two mentioned categories (DI lifecycle and contexts of usage) are tested and evaluated using the AHP method. Section 6 tries to introduce a summary table of the most important DI lifecycle and context of usage parameters of DIMS, and prioritise them by considering their role in forensically ready DIMSs. This list of prioritised DIMS parameters will help future research and studies in the field of digital and network forensic investigation, leading to the development of forensically ready DIMSs by considering the security and privacy challenges.

2 Literature review

In order to prepare and introduce a set of important DI parameters for forensically ready DIMSs, above-mentioned core facets of evaluation criteria should be considered. Moreover, the DI lifecycle as well as context of usage parameters for those criteria that have important roles in DFI needs to be collected and reviewed. Identity rules as stated by Cameron (2005) can be summarised as Table 2.

Table 2 Identity rules

Study	*Parameters, definitions*
Cameron (2005)	*User control and consent*, technical identity systems must only reveal information identifying a user with the user's consent.
	Minimal disclosure for a constrained use, the solution that discloses the least amount of identifying information and best limits its use is the most stable long-term solution.
	Justifiable parties, digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.
	Directed identity, a universal identity system must support both 'omni-directional' identifiers for use by public entities and 'unidirectional' identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.
	Pluralism of operators and technologies, a universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.
	Human integration, the universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.
	Consistent experience across contexts, the unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

Source: Cameron (2005)

Obviously, a user's security and privacy parameters for DI lifecycle play important roles in DIMS to give assurance of safety and make them successful. For digital technology and internet usage to fully deploy their potential, it is crucial that strong protection of digital identity be achieved. El Maliki and Seigneur (2007) summarises user-centric digital identity parameters as shown in Table 3.

Table 3 Identity user-centric parameters

Study	*Parameters, definitions*
El Maliki and Seigneur (2007)	*Empowering the total control of users over their privacy.*
	Usability, since users use the same identity for each identity transaction.
	Giving a consistent user's experience thanks to uniformity of identity interface.
	Limiting identity attacks, (i.e. *phishing*)
	Limiting reachability/disturbances, spam reduction
	Reviewing policies on sides if required, identity providers and service provider's websites.
	Huge scalability advantages, since the identity provider does not have to get any prior knowledge about the service provider.
	Assuring secure conditions when exchanging data
	Decoupling digital identity from applications
	Pluralism of operators and technologies

Source: El Maliki and Seigneur (2007)

DIMSs must ensure that such information is not misused and the individual's privacy is guaranteed (Bertino et al., 2009). In the DFI process, a user's security and privacy parameters in the DI lifecycle involve the capabilities and characteristics of DIMS that help in DFI and collect digital evidence. Dhamija and Dusseault (2008) summarise some of the security and privacy parameters as shown in Table 4.

Table 4 Identity security and privacy parameters

Study	*Parameters, definitions*
Dhamija and Dusseault (2008)	*Identity management is not a goal itself*, identity management is rarely a user's primary goal. Users are focused on their primary tasks, and identity management systems should aim to facilitate those tasks seamlessly, securely, and privately.
	Cognitive scalability is as important as technical scalability, identity management scheme designers must be cautious about reducing one user's burden while simultaneously increasing users' total workload or mental overhead.
	Users follow the path of least resistance, for identity management systems to succeed, users must find them easy to configure and use correctly and securely. It is also important to integrate identity management into the operating system or browser, so that users do not need additional software or incur additional costs.
	User consent could lead to maximum information disclosures, asking users to consent to more transactions would not result in greater control of information disclosures in identity management systems. By asking them to manage more identity information and presenting them with more choices, we only overwhelm them. The end result could be a system that increases, rather than minimises, the identity data that users are willing to reveal to third parties.
	We need mutual authentication (not just user authentication), to ensure that users are not providing their passwords to a phishing site, they must be able to authenticate the SP web site to ensure that it can be trusted to redirect to the correct IdP, and they should also authenticate the IdP's website.
	SPs want to control the customer experience, many websites wish to control their own user accounts to monitor usage, prevent abuse of their services, and protect information about their customers. Designers must understand that the SP's motivations are distinct from that of users. So to be widely adopted identity management systems must cater to both.
	Trust must be earned (and is hard for users to evaluate), no organisation can ensure a completely trusted system, and any bad or careless actor can tarnish the reputation of many. Thus, the identity community as a whole has a responsibility to behave securely and call attention to practices that threaten privacy or are unsafe.

Source: Dhamija and Dusseault (2008)

Moreover, by considering different types of identity usage in secure banking transactions as stated in Barisch et al. (2010), privacy and security parameters for the DI lifecycle can be as listed in Table 5.

Table 5 Identity security and privacy parameters

Study	*Parameters, definitions*
Barisch et al. (2010)	*Overcome identity fragmentation*, user's digital identity is fragmented. Thus user attributes are distributed across various accounts with different SP. The users have to be supported to manage this highly distributed information by means of a unified view across systems and providers.
	Cross-Layer IdM, most IdM solutions target SSO for application layer services, neglecting the network layer with inconvenient and even dangerous consequences. In order to achieve cross-layer IdM, network authentication must be compatible with application layer authentication. That means we need an IdM solution that takes application layer as well as network layer into account.
	Improved privacy features, privacy preservation is one of the most important properties of IdM for user acceptability. The considerations of current research on privacy enhancing technologies need to take network properties into account, because network identifiers can be used for correlation.
	Support for multiple devices, current IdM solutions do not take into account that an end user owns more than one device and uses these devices to consume services. By providing an integrated view across all end user devices, taking into account the diversity of devices as well as of identities, the usability and security of IdM can be further increased.
	No dependency on online components, many IdM solutions depend on components like identity or attribute providers in order to work. That means these systems need 100% availability, which is difficult to guarantee. Moreover, if a user has no network connectivity, the system should still work for limited period of time. Therefore, solutions are needed that work temporarily without dependencies on online components.
	Backward compatibility, it is not reasonable to build new IdM solutions that do not interwork with already existing solutions. Therefore, new IdM solutions have to be either compatible with already existing systems or have to provide opportunities to interwork with those legacy systems.

Source: Barisch et al. (2010)

Many countries and international organisations (such as the European Union) have technical frameworks to enable users and citizens to have control over their identity and the identity information disclosure (Camenisch et al., 2005). DI lifecycle parameters to provide such legal framework for user's control over his/her identity information can be considered in Table 6.

Table 6 Digital identity legal framework parameters

Study	*Parameters, definitions*
Camenisch et al. (2005)	*User informed consent and control*, the user keeps control over which personal data are given to whom and for which purpose and maintains a complete and coherent view of the privacy policy of all their transaction partners.
	Privacy negotiation, when a user discloses personal data, the user can express a privacy policy which states how her personal data should be handled. *Data minimisation* – transaction partners only collect personal data that are necessary to perform their part of the transaction.

Source: Camenisch et al. (2005)

Table 6 Digital identity legal framework parameters (continued)

Study	*Parameters, definitions*
Camenisch et al. (2005)	*Identity management*, a user may also wish to release different amounts of personal information depending on the trustworthiness of the transaction partner. *Spectrum of anonymity*, at one end of the spectrum, the parties agree to proceed without the need for any identifying data and the relationship can stay anonymous. At the other end of the spectrum, in medium-to-high risk transactions and law-related transactions, a third-party-issued identity proof such as an identity card, or a witness like a notary might be necessary. *Accountability*, let us reiterate that properly-designed anonymous transactions can also provide accountability – in other words, a user can be made accountable for misuse of the system or cheating, even though transactions are 'anonymous'.

Source: Camenisch et al. (2005)

Moreover, Bonneau et al. (2012) define 25 properties for DI lifecycle evaluation in web services in three categories, namely usability, deployability, and security:

Table 7 Digital identity web services parameters

Study	*Parameters, definitions*
Bonneau et al. (2012)	*Usability parameters:* • *Memory wise-effortless*, users of the scheme do not have to remember any secrets at all. • *Scalable-for-users*, using the scheme for hundreds of accounts does not increase the burden on the user. • *Nothing-to-carry*, users do not need to carry an additional physical object (electronic device, mechanical key, piece of paper) to use the scheme. • *Physically-effortless*, the authentication process does not require physical (as opposed to cognitive) user effort beyond, say, pressing a button. • *Easy-to-learn*, users who do not know the scheme can figure it out and learn it without too much trouble, and then easily recall how to use it. • *Efficient-to-use*, the time the user must spend for each authentication is acceptably short. • *Infrequent-errors*, the task that users must perform to log in usually succeeds when performed by a legitimate and honest user. • *Easy-recovery-from-loss*, a user can conveniently regain the ability to authenticate if the token is lost or the credentials forgotten. *Deploy ability parameters:* • *Accessible*, users who can use passwords are not prevented from using the scheme by disabilities or other physical (not cognitive) conditions. • *Negligible-cost-per-user*, the total cost per user of the scheme, adding up the costs at both the prover's end (any devices required) and the verifier's end (any share of the equipment and software required), is negligible.

Source: Bonneau et al. (2012)

Table 7 Digital identity web services parameters (continued)

Study	*Parameters, definitions*
Bonneau et al. (2012)	• *Server-compatible*, at the verifier's end, the scheme is compatible with text-based passwords. • *Browser-compatible*, users do not have to change their client to support the scheme and can expect the scheme to work when using other machines with an up-to-date, standards-compliant web browser and no additional software. • *Mature*, the scheme has been implemented and deployed on a large scale for actual authentication purposes beyond research. • *Non-proprietary*, anyone can implement or use the scheme for any purpose without having to pay royalties to anyone else. *Security parameters:* • *Resilient-to-physical-observation*, an attacker cannot impersonate a user after observing them authenticate one or more times. • *Resilient-to-targeted-impersonation*, it is not possible for an acquaintance (or skilled investigator) to impersonate a specific user by exploiting knowledge of personal details (birth date, names of relatives etc.). • *Resilient-to-throttled-guessing*, an attacker whose rate of guessing is constrained by the verifier cannot successfully guess the secrets of a significant fraction of users. • *Resilient-to-unthrottled-guessing*, an attacker whose rate of guessing is constrained only by available computing resources cannot successfully guess the secrets of a significant fraction of users. • *Resilient-to-internal-observation*, an attacker cannot impersonate a user by intercepting the user's input from inside the user's device (e.g., by key logging malware) or eavesdropping on the clear text communication between prover and verifier [we assume that the attacker can also defeat TLS if it is used, perhaps through the certificate authority (CA)]. • *Resilient-to-leaks-from-other-verifiers*, nothing that a verifier could possibly leak can help an attacker impersonate the user to another verifier. • *Resilient-to-phishing*, an attacker who simulates a valid verifier (including by DNS manipulation) cannot collect credentials that can later be used to impersonate the user to the actual verifier. • *Resilient-to-theft*, if the scheme uses a physical object for authentication, the object cannot be used for authentication by another person who gains possession of it. • *No-trusted-third-party*, the scheme does not rely on a trusted third party (other than the prover and the verifier) who could, upon being attacked or otherwise becoming untrustworthy, compromise the prover's security or privacy. • *Requiring-explicit-consent*, the authentication process cannot be started without the explicit consent of the user. • *Un-linkable*, colluding verifiers cannot determine, from the authenticator alone, whether the same user is authenticating to both.

Source: Bonneau et al. (2012)

By considering organisational information processes along with the client's roles and responsibilities in an organisational chart, identity parameters should be considered and listed for future evaluation. Based on the IdM expertise point of view, Hall and Liedtka (2007) and GenericIAM (2007) summarised the following parameters as evaluation parameters for DI lifecycle for IdM in an organisation (Table 8).

Table 8 Most prevalent factors for implementing IdM in organisations

1 Risk management/IT security goal
• Minimise liabilities
• Mitigate risks
• Make systems more secure
2 Value creation goals
• Efficiency goals (e.g. process optimisations)
• Lower overall costs
3 Compliance goals
• Comply with relevant laws and regulations [e.g. Basel II or Sarbanes-Oxley Act (SOX)]

Source: Based on Hall and Liedtka (2007) and GenericIAM (2007)

This paper sought to survey and review related articles and literature on the DI lifecycle and context of usage by considering its role as DF, and discussion about the importance of DI as DF (Leskinen, 2012) has tried to evaluate DIMS parameters by considering its functioning in different usage contexts. Other articles dealing with DF have tried to introduce DFIM and its trend to propose an integrated model (Kohn et al., 2013) to collect digital evidence and analyse them. It seems there is no such approach and classification regarding DI lifecycle parameters in DIMS that consider its role and affect each components of the digital investigation process.

You can find below summary list of DI lifecycle and context of usage parameters in forensically ready DIMS which have been proposed in reviewed studies (Table 9).

Table 9 Comparison of DI parameters studies for forensically ready DIMS

Criterions / *Study*	*1*	*2*	*3*	*4*	*5*
Cameron (2005)	-	✓	-	✓	✓
El Maliki and Seigneur (2007)	✓	✓	-	✓	-
Dhamija and Dusseault (2008)	✓	✓	✓	-	-
Barisch et al. (2010)	-	✓	-	✓	-
Camenisch et al. (2005)	-	✓	-	✓	-
Bonneau et al. (2012)	-	✓	✓	-	✓
Hall and Liedtka (2007) and GenericIAM (2007)	-	✓	✓	-	-

Notes: Criterions: 1 – user-centric identity paradigm; 2 – user's security and privacy; 3 – user's legal perspective; 4 – types of DIMSs; 5 – type of application (context of usage)

According to the related literature and research papers that compare forensically ready DIMS criteria, it becomes apparent that there is no previous study that evaluates and prioritises DI life cycle and the context of usage parameters.

3 Classifying DI lifecycle parameters

The following parameters and evaluation criteria of DIMS are presented based on the parameters discussed in the literature review, while also taking into account the DI lifecycle application in DFI.

As explained in Section 1 of present paper, it is important to evaluate and prioritise DI lifecycle parameters by considering its role as important digital evidence in DFI, so a priority list of DI lifecycle parameters in DIMS that affect the DFI process will be provided.

According to DFIM phases and also considering our goal to develop and use a forensically ready DIMS, those DI lifecycle parameters that help us collect maximum DI information as digital evidence with minimum DFI costs in each of the four DFIM phases should be considered. For example, in the first phase of integrated DFIM, it seems DI lifecycle parameters that provide more and optimised control over DI information transactions and help us keep proper logging of DI information in DIMS (i.e. time stamp, mutual authentication protocols) should appear at the top of our evaluation list.

This paper initially tried to categorise and list the most important DI lifecycle parameters in DIMS by reviewing them based on experts' views. It also shed light on DI information as digital evidence in DFI in the investigation into present-day computer and internet-related crimes. In the next phase, a basic list of DI lifecycle parameters based on the results of the evaluation process will be considered for forensically ready DIMSs.

3.1 Classifying DI parameters by considering contexts of usage

This section provides a list of DI parameters by considering contexts of usage of DIMS and the role of DI information as digital evidence in DFI.

Obviously when talking about DFI process and DFIM phases and trying to build a forensically ready system, the context of usage is an important issue that affects federated DIMS architecture, security, and privacy properties. Therefore, to build a proper list of DI parameters by considering their role in DFI, challenges of usage contexts should be taken into account (i.e. the type and environment of web applications) to evaluate our DI parameters and try to develop and use a forensically ready DIMS. For example in the second phase of our DFIM, which is the deployment phase, it seems that DI parameters which help us detect a crime in an optimised way and in a low-cost online hospital IS system, such as online and offline data acquisition and traffic capturing, parameters of staff knowledge and expertise, should be placed at the top of our list of DI parameters. DI parameters in DIMS by considering contexts of usage and DI role as digital evidence in DFI process will be presented in the next section.

After this, a list of parameters that should be considered to make forensically ready DIMS will be evaluated.

4 Evaluating DI parameters

4.1 Evaluating DI lifecycle parameters

This section attempts to evaluate the proposed DI lifecycle parameters in DIMS, which we had identified in Section 3. For this purpose, five experts including assistant professors at a cyberspace institute, independent IT and ICT experts to the Court and IT managers were requested to give their opinions via online questionnaires (http://www.network-forensic.net/form/PID01-09). DI lifecycle parameters using the AHP evaluation method, which has been prioritised in this paper, can be found in Table 10. Moreover, the weight of each DI lifecycle parameter has been presented in Figure 1.

Table 10 AHP evaluation outcome of DI lifecycle parameters in DIMS forensic ready

Ranking	*DI lifecycle parameters*
1	Minimal disclosure for a constrained use
2	Directed identity
3	Justifiable parties
4	Users follow the paths with least resistance
5	User control and consent
6	Consistent experience across contexts
7	Giving a consistence user experience
8	Continues trust and risk assessment
9	Pluralism of operators and technologies
10	Usability
11	Cognitive scalability
12	Human integration
13	Relying parties want to control customer experience
14	Mutual authentication, not just user authentication

4.2 Evaluating DI contexts of usage parameters

This section tries to evaluate the proposed DI contexts of usage parameters in DIMS, which we identified in Section 4. For this purpose, five experts including assistant professors at a cyberspace institute, independent IT and ICT expert engineers to the Court and IT managers were requested to give their opinion via online questionnaires (http://www.network-forensic.net/form2/PID02-04). Prioritised DI contexts of usage parameters using the AHP evaluation method can be found in Table 11. Besides, the weight of each DI context of usage parameter has been presented in Figure 2.

Figure 1 DI lifecycle parameters in forensically ready DIMS (see online version for colours)

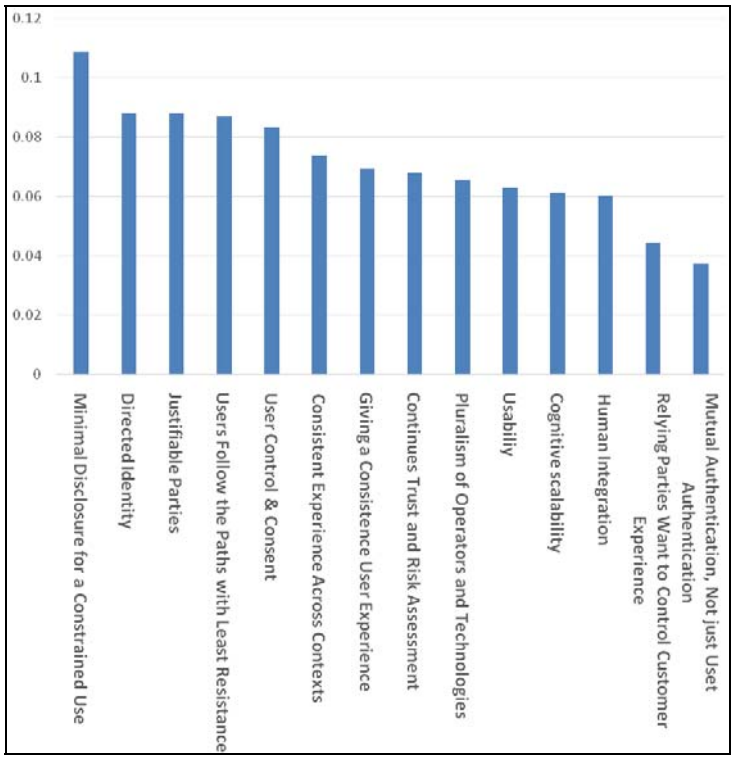
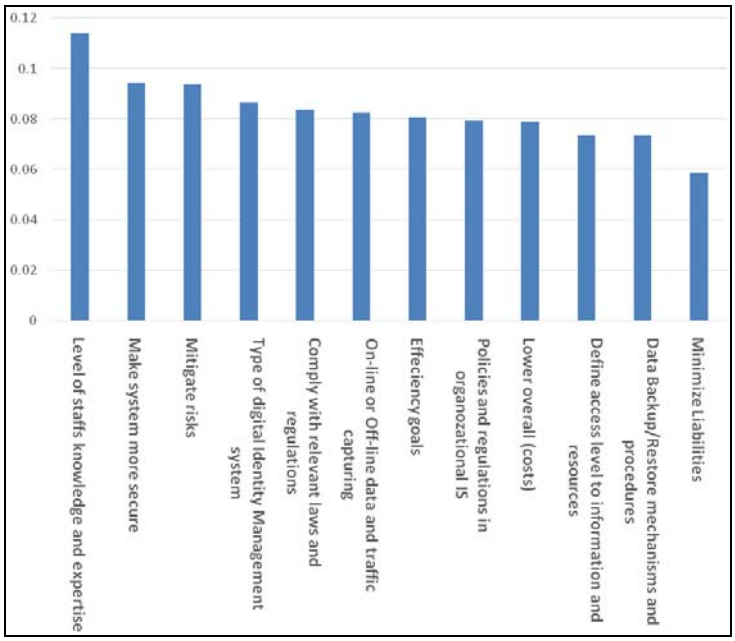


Table 11 AHP evaluation outcome of DI contexts of usage parameters in DIMS forensic ready

Ranking	*DI contexts of usage parameters*
1	Level of staffs knowledge and expertise
2	Make system more secure
3	Mitigate risks
4	Type of DIMS
5	Comply with relevant laws and regulations
6	On-line or off-line data acquisition and traffic capturing
7	Efficiency goals
8	Policies and regulations in organisational IS processes
9	Lower overall (costs)
10	Defined access levels to information and resources
11	Data backup/restore mechanism and procedures
12	Minimise liabilities

Figure 2 DI contexts of usage parameters in dims forensic ready (see online version for colours)



5 Disscussions and conclusions

The growing-use of cyberspace applications and the increasing number of online services have resulted in a sharp increase in the occurrence of cyber-attacks attacks and computer-related crimes. This increase in the incidence of cyber-crimes necessitates new solutions and tools to deal with these crimes. Digital crime investigations are based on digital evidence gathered from the crime scene. Crime scenes in digital crime investigation are the cyber space and computer networks.

This paper proposed a new set of evaluation and design criteria for future DIMS that is forensically ready based on existing criteria and relevant literature about the identity management application areas in digital forensic investigation.

Our evaluation revealed that while the criteria already give promising results, this could be improved by creating a more fine-grained set of parameters under each current criterion, thereby enabling more detailed results for forensically ready DIMS and improving DIMS development for a complete DFI process.

The evaluation revealed some issues related to current DIMSs. These issues were the DI lifecycle parameters such as *minimal disclosure for a constrained use, directed identity, justifiable parties, users' following the paths with least resistance, and user control and consent. These most important DI lifecycle parameters show that in cases of DF and DFIP which are related to users' security, privacy, and legal aspects in cyber space applications, minimum personal information for known purpose and usage are the most important parameters. Also this list can be used as a reference for professional and experienced IT users, indicating concerns and challenges regarding digital identity in the*

development of DIMS. The DI context of usage parameters such as staff knowledge and expertise, making systems more secure, risks mitigation, type of DIMS, and compliance with relevant laws and regulations also supports the forensic readiness of DIMS. These parameters reveal the necessity and effectiveness of providing to the staff proper and adequate information about DFI and the relevant laws and regulations governing DIMS. Moreover, they will help to successfully develop and use forensically ready DIMS and reduce DFIP risks.

These parameters seem to stem from the importance of designing identity management systems to function in secure and private manner and as a forensically ready system in DFIM.

6 Further study

Future work needed in this area to further elaborate the evaluation criteria and provide a more extensive evaluation of the existing identity systems as a digital forensically ready system. In order to improve on the proposed parameters to cover all aspects of cyberspace applications and their DIMSs, it is necessary to consider and evaluate parameters that are related to various types of networks and communication environments, along with the security level of information and the required type of access control in our IS.

The evaluation of the current systems should be applied to actual systems in DFIM, and the test parameters and groups should be used in the actual evaluation in order to produce more comprehensive and accurate results.

References

Agarwal, A. et al. (2011) 'Systematic digital forensic investigation model', *International Journal of Computer Science and Security (IJCSS)*, Vol. 5, No. 1, pp.118–131.

Alpár, G. et al. (2011) *The Identity Crisis. Security, Privacy and usability Issues in Identity Management*, arXiv preprint arXiv:1101.0427.

Barisch, M. et al. (2010) 'Security and privacy enablers for future identity management systems', *Future Network and Mobile Summit*, IEEE.

BBC News (22 July 2007) 'Web networkers 'at risk of fraud'' [online] http://news.bbc.co.uk/2/hi/uk_news/6910826.stm.

Banihashemi, S., Homayounvala, E., Talebpour, A. and Abhari, A. (2016) 'Identifying and prioritizing evaluation criteria for user-centric digital identity management systems', *International Journal of Advanced Computer Science & Applications*, Vol. 1, No. 7, pp.45–54, DOI: 10.14569/IJACSA.2016.070707.

Berghel, H. (2005) 'The two sides of ROI: return on investment vs. risk of incarceration', *Communications of the ACM*, Vol. 48, No. 4, pp.15–20.

Bertino, E. et al. (2009) 'Digital identity protection-concepts and issues', *4th International Conference on Availability, Reliability and Security*, Fukuoka, Japan.

Bonneau, J. et al. (2012)' The quest to replace passwords: a framework for comparative evaluation of web authentication schemes', *Security and Privacy (SP), IEEE Symposium on*, IEEE.

Camenisch, J. et al. (2005) 'Privacy and identity management for everyone', *Proceedings of the Workshop on Digital Identity Management*, ACM.

Cameron, K. (2005) 'Laws of identity'.

Cao, Y. and Yang, L. (2010) 'A survey of identity management technology', *Information Theory and Information Security (ICITIS), IEEE International Conference on*, IEEE.

Casey, E. (2001) *Handbook of Computer Crime Investigation: Forensic Tools and Technology*, Academic Press.

Dabrowski, M. and Pacyna, P. (2008) 'Generic and complete three-level identity management model', *Emerging Security Information, Systems and Technologies, SecureWare, Second International Conference on*, IEEE.

Dhamija, R. and Dusseault, L. (2008) 'The seven flaws of identity management: usability and security challenges', *Security & Privacy*, IEEE, Vol. 6, No. 2, pp.24–29.

El Maliki, T. and Seigneur J-M. (2007) 'A survey of user-centric identity management technologies', *Emerging Security Information, Systems, and Technologies, SecureWare, The International Conference on*, IEEE.

Endicott-Popovsky, B. et al. (2007) 'A theoretical framework for organizational network forensic readiness', *Journal of Computers*, Vol. 2, No. 3, pp.1–11.

Francia, G.A. and Clinton, K. 'Computer forensics laboratory and tools', *Journal of Computing Sciences in Colleges*, Vol. 20, No. 6, pp.143–150.

GenericIAM (2007) 'Processes of identity and access management' [online] http://www.genericiam.org/.

Hall, J.A. and Liedtka, S.L. (2007) 'The Sarbanes-Oxley Act: implications for large-scale IT outsourcing', *Communications of the ACM*, Vol. 50, No. 3, pp.95–100.

Hansen, M. and Meints, M. (2006) 'Digitale Identitäten – Überblick undaktuelle Trends', *Datenschutz und Datensicherheit (DuD)*, Vol. 30, No. 9, pp.571–575.

Ieong, R.S. (2006) 'FORZA – digital forensics investigation framework that incorporate legal issues', *Digital Investigation*, Vol. 3, pp.29–36.

Independent Center for Privacy Protection (ICPP) and Studio Notarile Genghini (SNG) (2003) 'Identity management systems (IMS): identification and comparison study'.

Jones, A. and Martin, T. (2010) *Digital Forensics and the Issues of Identity*, Information Security Technical Report, Vol. 15, No. 2, pp.67–71.

Jøsang, A. et al. (2007) 'Usability and privacy in identity management architectures', *Proceedings of the Fifth Australasian Symposium on ACSW Frontiers*, Australian Computer Society, Inc., Vol. 68.

Köhn, M. et al. (2008) *UML Modelling of Digital Forensic Process Models (DFPMs)*, ISSA, Citeseer.

Kohn, M.D. et al. (2013) 'Integrated digital forensic process model', *Computers & Security*, Vol. 38, pp.103–115.

Kruse II, W.G. and Heiser, J.G. (2010) *Computer Forensics: Incident Response Essentials*, Pearson Education.

Lee, H. et al. (2009) 'Criteria for evaluating the privacy protection level of identity management services', *Emerging Security Information, Systems and Technologies, SecureWare, Third International Conference on*, IEEE.

Leskinen, J. (2012) 'Evaluation criteria for future identity management', *Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 11th International Conference on*, IEEE.

Maler, E. and Reed, D. (2008) 'The Venn of identity: options and issues in federated identity management', *IEEE Security & Privacy*, Vol. 2, pp.16–23.

Mezler-Andelberg, C. (2008) *Identity Management*, eine Einführung, dpunktVerlag.

Mueller, M.L. et al. (2006) 'Digital identity: how users value the attributes of online identifiers', *Information Economics and Policy*, Vol. 18, No. 4, pp.405–422.

Ngobeni, S. et al. (2010) 'A forensic readiness model for wireless networks', *Advances in Digital Forensics VI*, Springer, pp.107–117.

Perez, S. (2009) *Fake Social Network Profiles: a New Form of Identity Theft in 2009*, ReadWriteWeb.

Saaty, T.L. (2008) 'Decision making with the analytic hierarchy process', *Int. J. Services Sciences*, Vol. 1, No. 1, pp.83–98.

Spantzel, B. et al. (2006) *User Centricity: A Taxonomy and Open Issues*, IBM Zurich Research Laboratory.

Tan, J. (2001) *Forensic Readiness*, pp.1–23, Stake, Cambridge, MA.

Wayman, J.L. (2008) 'Biometrics in identity management systems', *Security & Privacy*, IEEE, Vol. 6, No. 2, pp.30–37.

Windley, P.J. (2005) *Digital Identity*, O'Reilly.