

**SECURITY** Identity management is key in controlling corporate risk and meeting regulatory requirements. The trick is to find a solution that works any time, any place

## Putting the identity pieces together

Neil Macehiter  
Tech Talk



Identity data plays a key role in facilitating trust in business and contractual relationships. It is one aspect of the information that subjects use to assess the level of risk associated with participating in activities.

For example, an online bank demands identifying information to assess whether it is willing to allow an individual to view the balance of an account, and it may require additional information for the transfer of funds between accounts, reflecting the relative risks associated with the two transactions.

It is worth clarifying what we mean by identity. According to the Oxford English Dictionary, identity is "the fact of being who or what a thing or person is". Identity is the set of characteristics and attributes, including names, biometric characteristics, relationships and roles which serve to identify in a particular context.

For example, the fact that someone is over 18 in the UK is sufficient to identify them in the context of purchasing alcohol, while their name, job role and employee number are required to identify them in the context of updating their personnel details in the human resources system at their place of employment.

Identity attributes can manifest themselves in physical and digital forms, such as a driving licence and an employer-issued smartcard. It is important to recognise that we are talking about the digital representation of the attributes, or more correctly the claims to possessing the attributes made by the subject, which serve to identify a person or thing - a digital identity.

Identity management can be regarded as the set of processes and supporting technologies which together manage the electronic definition, storage and lifecycles of digital identities and associated policies. It is also the application of those identities and policies to establish trust in the exchange of electronic information between multiple parties.



Who are you? Credentials must fit to prove a subject's claim to an identity

### KEY POINTS

- ▶ Identity management has key role in compliance and operational efficiency
- ▶ Organisations have a wide array of identity-centric requirements
- ▶ The broad picture shows the same capabilities needed in different scenarios
- ▶ Firms will increasingly need to bring together all of these capabilities

Closely related to the notion of identity is that of credentials. Credentials are used to prove a subject's claim to possess a particular identity, and thus contribute to the ability of one digital subject to trust another. Credentials typically comprise one or more of:

- Something you know, for example a password
- Something you have, for example a smartcard
- Something you are, for example a fingerprint.

To access an online bank account, the bank requires a series of credentials, such as a personal identification number and a password, to be able to trust that an individual is who they claim to be.

The level of trust required, and thus the required credentials, depends on the context in which the digital identity is being used, although credentials in the real world are often used out of context.

An example of this mismatch is the use of a driving licence to validate the identity of an individual who wants to perform a currency

exchange transaction in a UK post office. Having a driving licence does not prove an individual's financial trustworthiness, and thus the credentials are out of context.

For the IT director, implementing an identity management strategy can be a daunting task. It is difficult to get an end-to-end view as organisations are faced with an array of trends, both business and IT, which require these capabilities. Identity management has a role to play in regulatory compliance, operational efficiency, cost reduction and improving information access.

Any strategy for identity management needs to consider online service provision, dealing with identity theft, privacy legislation and best practice privacy management. The IT director also needs to think about identity card initiatives and how identity management works within business collaboration with third-party companies.

The relative priority that different organisations place on these trends varies a lot and is dependent on a wide variety of factors. How-

ever, the trends are clearly broadly applicable and will be implemented by many enterprises over time. What is equally clear is that they have far-reaching implications for both business and IT.

The multiple trends lead to particular perspectives on the concept of identity management and different initiatives can lead to particular identity management perspectives.

In particular, some trends lead to perspectives of identity management that focus on how identities are managed, whereas others focus on how identities are used. Other trends focus on an enterprise's own domain of control, whereas others focus on a broader, external perspective of identity.

All of these trends are part of the broader identity management challenge, and you need to understand the whole to be able to understand your technology requirements.

Many of the elements that underpin identity management are mature and well understood and have an important role to play if organisations are to respond to the confusing array of identity-centric requirements. In particular, the following technologies are well understood:

- Authentication and credential management
- Authorisation and access control
- Directories
- Identity lifecycle management
- Logging and audit
- Self-service password management and provisioning
- Identity federation.

However, identity management suppliers are selling products that address very particular requirements, and pulling together particular technologies to support those requirements, but the broader picture of identity management reveals that the same capabilities are required over and over again across many different usage scenarios.

The upshot of this is that organisations will increasingly have to bring together all of these capabilities in an organised fashion - something that a lot of today's identity management products do not do well.

● Neil Macehiter is a partner at advisory company Macehiter Ward-Dutton

→ [www.mwdadvisors.com](http://www.mwdadvisors.com)