Managing Identity Trust for Access Control

by Gerrit J. van der Geest and Carmen de Ruijter Korver

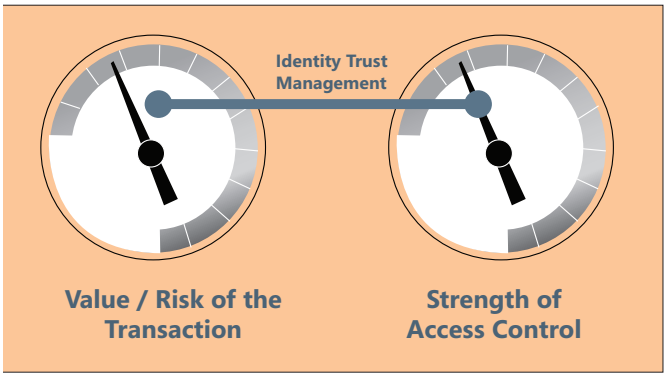
Summary

In the past, systems were used by a small set of users, mostly within the trusted circle of their organization. The circle of trust has, however, widened considerably. Today's computer systems are used by a variety of users across many organizations and geographical areas and via different channels. Organizations must make their information assets available to many users but simultaneously protect these against unauthorized access. However, each transaction that is used to access those information assets should bear just the appropriate level of access control, not too little in view of the security risks and not too much in view of user friendliness and high costs. How can we achieve an optimal balance between availability and protection?

The answer lies in the management of identity trust. We need to be able to create, maintain, and communicate various levels of trust. When we can manage identity trust effectively, we can subsequently tune the level of appropriate access control to the level of value or risk that is associated with the transactions (see Figure 1). An organization should therefore ensure that its strategic Identity and Access Management (IAM) architecture provides for mechanisms to capture and transport identity trust throughout the service layers within its IT infrastructure.

This article describes the management of identity trust as defined in an IAM reference architecture. It supports an organization's business requirements, which can range from providing low-threshold access for registration to performing high-risk financial transactions for high volumes of consumers. We'll introduce the concepts of identification trust, authentication trust, reputation trust, session trust, and trust level up- and downgrades. Additionally, we'll discuss how to implement such a model as part of a Service Oriented Architecture (SOA) by making use of the available industry standards.

Figure 1: Identity Trust Management



Challenges

Organizations face a number of challenges with respect to their Access Control:

Scalability. The e-business portfolio of organizations will strongly expand and new e-business services that require a high level of protection against fraudulent activities will have to be supported. This requires IAM functionality that is scalable from a quantity perspective and, even more important, from a security perspective.

Cost reduction. The implementation and management of adequate IAM functionality is a costly exercise. Organizations aim for sharing IAM functionality between their businesses.

Federation. Organizations will enter into more partnerships in which the partners may take responsibility for part of the IAM services based on a well-established trust relationship between the organization and these partners. On the other hand, identification processes are expensive and organizations that have implemented these processes can benefit by providing services to other organizations.

Client-centricity. Organizations want to be considered "easy to do business" with. Concepts like client-centricity are therefore important. Even organizations comprising extremely loosely coupled businesses and their partners must offer cross-business product portfolios to their consumers. Many cases require a group portal strategy for this purpose. Such a strategy can only succeed when it is supported by IAM services, which ensure that identity and authentication information can be exchanged between businesses without compromising their autonomy.

SOA compliance. Within an SOA architecture, the business processes are enabled via loosely coupled, coarse-grained, and reusable business services. The business services are exposed via technical interfaces based on industry open standards. The reusability of the services can only be achieved when appropriate controls are in place for protecting and ensuring service availability. Access Control information must

be communicated between service consumers, service providers, and between all enterprise components that make up the services. Traditionally, Access Control functionality was part of and integrated within several IT infrastructure components like operating systems, applications, and network components; the challenge will now be to implement this functionality as shared IAM services integrated within the Enterprise Service Bus.

Trust, Trust, Trust...

Only effective communication of IAM information such as identities, authentication assertions, or access policy decisions can address all of the challenges mentioned so far. Communication of IAM information requires the establishment of *trust* between the parties involved.

As described by the International Telecommunications Union, an entity can be said to "trust" a second entity when it (the first entity) has reason to assume that the second entity will behave exactly as the first entity expects.

Trust relationships are sometimes obscured but in essence exchange of information (not data) can only succeed based on some form of direct or indirect trust between the communicating parties. This applies in particular to the IAM information that is used for the protection of the resources, the assets of the organization. Transactions in IT systems, whether business, IAM, or technical transactions, represent some value or risk for the organization. Compromising a transaction may result in illegal access to a protected resource, which may lead to financial, reputation, or other types of losses.

In developing strategic IAM architectures, it became clear that we must formalize the trust concept in order to address the various challenges. In our model, the behavior as described in the definition is determined by policies established between the two entities. The level to which the receiver is able to trust the information received is dependent upon:

- the correctness of the way the policy was executed, and
- the policy that was agreed upon to generate the information.

Our Trust Model captures these two items by means of so-called Trust Levels. These Trust Levels are quantifiable and verifiable and can therefore be communicated between parties. The model requires an established governance framework.

Does Absolute Trust Exist?

This question should probably be answered by philosophers, but in the reference frame of Access Control, the answer is no. However, the absence of absolute trust does not bother us because we don't need it. In fact, we do not want it because of the disadvantages associated with obtaining higher levels of trust such as additional costs and inconvenience for users.

IAM's main objective is to provide Access Control to protected resources. The level of Access Control must be commensurate with the level of value/risk of the transactions executed against the protected resource. A level of protection that is too stringent for the type of transaction may result in high costs or bad user experience. A level of protection that is too low will increase the risks associated with the transactions. In other words, *we need to be able to create, maintain, and communicate various levels of Trust in order to tune the level of Access Control to the value/risk of the IT transactions involved.*

Trust Model

The IAM reference architecture includes a model that allows for such required commensuration of the level of Access Control to the value/risk of the IT transactions (see Figure 2). The core of this Trust Model consists of:

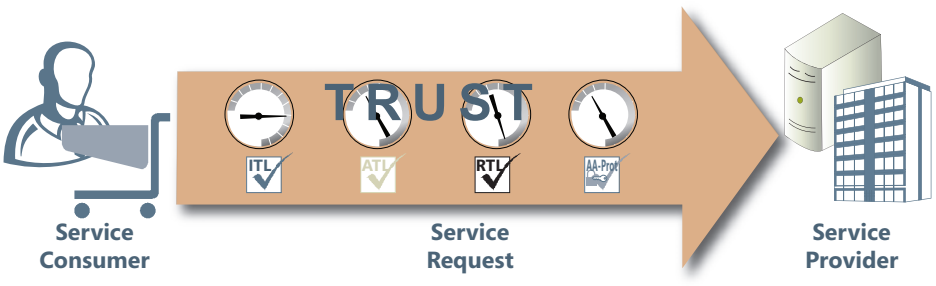
- A classification of the *IT transactions into value/risk categories* (four to six categories are often sufficient).
- Definition of *four IAM parameters* and appropriate levels to capture and communicate Trust:
  1. *Identification Trust Level (ITL)*
  2. *Authentication Trust Level (ATL)*
  3. *Reputation Trust Level (RTL)*
  4. *Level of protection of the Authentication Assertion.*
- *Associations* of the value/risk transaction categories with the parameter levels for the various Subject Types and Roles.
- Definition of mechanisms to *communicate* the parameter levels between the various infrastructure components involved in the execution of the IT transactions; and definition of mechanisms to *enforce* the required parameter levels by the resource in order to grant access.

Let's take a closer look at the four IAM parameters.

Parameter 1 - Identification Trust Level. To explain the ITL parameter, we'll first define some terminology. The terms are capitalized.

- ***Subject.*** Subjects access protected Resources. A Subject is a person, computer, device, service, or other entity that has, or will be provided, access to Resources, or has accessed Resources in such a way that audit records still have to be kept.
- ***Subject roles.*** In accessing Resources, a Subject can take on different Subject Roles. For example, a Subject of type 'Person' can assume the Subject Role of 'Personnel' but also the Subject Role of a 'Client'. In other words, employees can act on behalf of the organization in doing their daily work or act on behalf of themselves as clients of the organization procuring products or services.
- ***Digital identity.*** For a Subject to access a Resource, it must claim a Digital Identity (of type Security Principal). A Digital

Figure 2: Trust model



"IDENTIFICATION IS THE PROCESS OF VERIFYING THE CLAIMED IDENTITY OF A SUBJECT AND ASSIGNING A DIGITAL IDENTITY TO THE SUBJECT."

Identity is the representation of a Subject in the digital realm. A Digital Identity is a collection of related electronic data that represents the Assertions made by an Authority about the Subject. The Digital Identity is intended for use as a proxy of the Subject. There are various types of Digital Identities.

- ***Identification.*** Identification is the process of verifying (at a certain level of surety) the claimed Identity of a Subject and assigning a Digital Identity to the Subject. The Subject receives Credentials. Parties establish a contract (Identification Contract) during Identification.

  An Identification Authority or Identification Agent performs the Identification. The Identification Authority applies an Identification Policy in order to identify a Subject. The Identification Policy dictates the steps that the Authority needs to perform. A typical example of such steps are: the Authority physically meets the Subject, verifies his or her passport, and makes a copy (please note that there is also a trust relationship here with the Authority that issued the passport). The Identification Policy also defines the way the Credentials are distributed to the Subject. This is a strong Identification Policy that may be applicable to high-risk business transactions. For a low-risk business transaction, another Identification Policy may be applicable that only prescribes that the Subject must provide a valid e-mail address and that the Credentials are sent to that e-mail address. Typical examples of Identification Authorities are a PKI Certificate Authority, an authorized human resources employee, front desk employee, or even automated processes.

  Identification processes are expensive and may require manual interaction and involvement of third parties. They may also require involvement of the clients and tend to be experienced as unfriendly. So define and, if possible share, the most optimal process (do just enough) within or across organizations.

  The strength of the Identification is mainly related to the strength of the verification steps (policy) performed by the Identification Authority. This strength is reflected as so-called Identification Trust Level and represents the level of assurance in the authenticity and integrity of a Subject's claimed (legal) identity (the assurance that the Digital Identity represents the Subject).

  The ITL serves multiple purposes. In addition to the role it plays in Access Control, it is required for identity associations. Organizations often have multiple Digital Identities for the same Subject. In many cases, this is an undesirable situation. The processes to associate these Digital Identities — initiated by the organization but preferably driven by the Subject — will rely on the ITLs assigned to the various Digital Identities.

Parameter 2 - Authentication Trust Level. Authentication verifies and confirms a Subject's asserted Digital Identity with a specified or understood level of confidence. Credentials issued as a result of Identification are used as proof that the Subject has the right to claim the Digital Identity.

There are various strength levels for the Credentials, such as single factor username/password and more stringent forms like multifactor username/password combined with smartcards or biometrical traits. The Authentication strength is also dependent on the controls applied when establishing the session with the Subject and aspects like the channel, device type, location, and time also influence the strength of the Authentication.

The ATL represents the current session's Authentication strength. The Authentication Authority (which was involved in the verification of the provided Credentials) determines the ATL.

Parameter 3 - Reputation Trust Level. Reputation Trust represents a party's expectation that another party will behave as assumed, based upon past experience. Reputation Trust is bidirectional and can be split into Consumer Reputation Trust and Provider Reputation Trust.

The type of transactions performed, authentication history, and so on, can influence the Consumer Reputation Trust. The Consumer Reputation Trust is a dynamic parameter and can vary within a session. Consumer Reputation Trust will become an important parameter, and provisions in the IAM architecture capture, maintain, and communicate the RTLs; however, the exact definition is dependent on the specific situation and still subject to further investigation.

A client performing an e-business transaction will also implicitly establish a Provider Reputation Trust regarding the e-business provider. An e-business provider must strive towards a situation in which the Provider Reputation Trust as perceived by the client, commensurates the value/risk level of the transaction; for example, by the use of Extended Validation SSL Certificates and personalized welcome messages for higher risk transactions.

In this article, we focus on the consumer side of the Reputation Trust. The three parameters discussed so far (ITL, ATL, and RTL) need to be communicated between the service consumer and provider. Parameter 4 guarantees their integrity and authenticity at an appropriate level.

Parameter 4 - Protection of the Authentication Assertion. A protected Resource or Service Provider needs to receive an Authentication Assertion (security token), which allows it to enforce Access Control policies to determine if and to what extend it will grant access to its services. The enforcement of the Access Control policies may be delegated to a 'centralized' Policy Enforcement Point (PEP) supported by Policy Decision Points (PDP).

In the model, the Authentication Assertion contains Identity information combined with the ITL, ATL, and RTL and possibly other attributes such as privilege attribute certificates, to enable subsequent authorizations. The Identity information contained within the Authentication Assertion may reference various types of Digital Identities:

- ***Persistent identity.*** The Digital Identity originally claimed by the Subject at Authentication (also referred to as 'proclaimed identity').
- ***Implied identity.*** The Digital Identity used by intermediate services to access 'lower level' services in a trusted subsystem model.
- ***Initiating identity.*** A Digital Identity representing the person initiating the transaction. The need for such an identity is apparent in the following scenario: A client instructs a service desk employee to perform a transaction against his/her account. The persistent identity

represents the service desk employee. However, the identity of the client also needs to be kept and communicated. This identity is called the 'initiating identity'.
- ***Domain identity***. A Digital Identity associated with the Subject within a dedicated application or business domain.

The Authentication Assertion requires protection because it contains information that must not be compromised while stored or in transport. The authenticity and integrity of the Authentication Assertion is crucial, while the confidentiality of the Authentication Assertion is in most cases less important, regardless the fact that integrity may be enhanced by applying confidentiality (security by obscurity).

Protection of the Authentication Assertion is a considerable cost factor due to the required processing needed for encrypt and decrypt technologies. Therefore, the protection should be tuned to the value/risk levels of the transactions. In some cases, an SSL/TLS or IPsec transport layer security will suffice, while other situations require message layer security by applying WS-Security with various encryption levels.

The IAM reference architecture defines three levels for the protection strength of the Authentication Assertions. The service provider needs to enforce, by means of its policies, that the required level has been applied.

Associating Value/Risk Transaction Levels with the Parameter Levels

After they have been defined, it is possibe to associate the various transaction value/risk levels and parameter levels. This needs to be done for each Subject Type and Subject Role. For example, the mapping for a Subject of Type 'Person' in Role 'Personnel' will differ from a Subject of Type 'Person' in Subject Role 'Client'. Their identification policies, the way they authenticate, and the transaction types, may all differ. It is also necessary and possible to include transactions in the model that are not directly related to the core business of the organization. This concerns transactions such as IT administrator transactions and IAM transactions for Subjects in Role 'Personnel'.

Figure 3 shows how you can associate the transactions to the ITL, ATL, RTL and Authentication Assertion Protection Levels for the Subject Role 'Client'.

In order to execute this specific transaction in the value/risk category 'Medium,' the following minimum parameters must be met:

- ITL C30 stands for: an Identification Policy that includes documented proof, copy of passport, Credential distribution by out-of-band mechanism.
- ATL 4 stands for: username and strong password combined with one-time PIN via cellphone.
- RTL 50 stands for: no incidents, no history yet.
- Authentication Assertion Protection level B stands for: transport layer security, AES 256 bits encryption.

Before we discuss how the Trust Model should be implemented, we must introduce the concept of Trust Level upgrades and downgrades.

Trust Level Upgrades and Downgrades

A protected Resource will enforce an Access Control Policy, which dictates that certain minimum levels of ITL, ATL, RTL, and Authentication Assertion protection must be met. If the levels are not appropriate, it rejects the service call and requires higher Trust Levels. This triggers a process requiring additional Credentials such as a PIN. This is called an ATL upgrade. Some IAM product suites support ATL upgrades.

ITL up- and downgrades are also possible. A typical example of an ITL upgrade is when an existing e-business client enrolls for higher risk transactions and is required to come to the office and provide a copy of his/her passport. The security principal that he/she uses will stay the same but it gets a higher ITL assigned. An ITL downgrade may occur when an Identification renewal process was not executed in time, or when some of the verifications executed during the initial Identification are no longer sufficient.

An RTL upgrade may happen when there is regular use and no incidents are reported over a certain time period. A (temporary) RTL downgrade may be the result of the fact that the user has lost part of his/her Credentials.

Implementation

The ITL, ATL, and RTL are combined into what is referred to as the *Session Trust object*. Listing 1 shows the structure (see page 16).

Session Trust is the level of surety that the Digital Identity wanting to transact actually originates from the Subject, whose identity information is linked to the Digital Identity, and that this Subject will behave in the agreed manner.

The Session Trust object must be communicated as part of service requests and forms part of the Security Token embedded within these requests. There are various alternatives, but consider the implementation in a Web Services environment in which the Authentication Assertion is formatted as an SAML Authentication Assertion (SAML element <AuthnStatement>). The <AuthnStatement> element provides a means to capture the Session Trust object via its definition of the Authentication Context (<AuthnContext>) element.

According to the SAML standard: *"A particular authentication context declaration defined in this specification will capture characteristics of the processes, procedures, and mechanisms by which the authentication authority verified the subject before issuing an identity, protects the secrets on which subsequent authentications are based, and the mechanisms used for this authentication."*

The <AuthnContext> element is extensible and provides the rudimentary structure to capture Session Trust. The

Figure 3: Associating value/risk transaction levels with the parameter levels

IT Transaction	Value/ Risk	ITL	ATL (Credential value only)	RTL	AuthN Assertion Protection
...	...	...	...	...	...
Transfer funds from current to savings account	**Medium**	**C30**	**4**	**50**	**B**
...	...	...	...	...	...

Listing 1: Structure of the Session Trust object

```
<Session Trust>
        <IdentificationTrust>nnn</IdentificationTrust>
        <AuthenticationTrust>
            <TypeOfCredentials>nnn</TypeOfCredentials>
            <Channel>nnn</Channel>
            <DeviceType>nnn</DeviceType>
            <Location>nnn</Location>
        </AuthenticationTrust>
        <ReputationTrust>nnn</ReputationTrust>
</Session Trust>
```

architecture prescribes an extension of this structure to cater to the full Session Trust object.

Suppose parameter 4 indicates that the Authentication Assertion must be protected by message layer protection. In that case, use the WS-Security standard and place the SAML Authentication Assertion in a <wsse:Security> element of the SOAP header. To meet the required authenticity and integrity requirements, the issuer or attesting entity will sign the Authentication Assertion and the encryption algorithm and key length must meet the complexity as defined for parameter 4.

The Service Provider needs to implement (WS-Policy) service policies to enforce compliance of the four parameter values to the IT transaction value/risk levels of the services that it provides. It will validate the ITL, ATL, and RTL and will only accept service requests that meet the required level of protection of the contained Authentication Assertion. If these levels are not met, it will inform the service consumer, which may initiate a Trust Level upgrade procedure to meet the required levels. The Service Provider may delegate some of this verification to a Security Token Service (STS), which may also cater to Security Token transformations based on its established trust relationships with Authentication Authorities.

"IT ALL BOILS DOWN TO THE WILLINGNESS OF THE PARTIES INVOLVED TO COOPERATE, TO ESTABLISH FORMAL AGREEMENTS FOR THIS COOPERATION, AND TO ADHERE TO THOSE AGREEMENTS."

The Session Trust object contains consolidated information about the executed Identification and Authentication process and changes that occurred in the Reputation. The information contained in the object is condensed in such a way to enable communication in various technology sets and protocols. Web Access environments may require implementation of the Session Trust object within the HTTP header, which has its length limitations.

More elaborated Access Control mechanisms need additional information on top of the Session Trust object. The IAM services maintain a so-called *Trace object*, which reflects all the detailed information about the performed Identification and Authentication process steps and Reputation changes.

Listing 2 provides a possible structure for the Trace object.

The Identity Services will maintain the first and last part, while the Authentication Authorities will cater to the second part. The Trace object also plays an important role in auditing the IAM processes.

Note that the object caters to multiple Identification and Authentication steps and Reputation changes to register Trust Level upgrades and downgrades. The Trace object is associated with the unique identifier assigned to the Digital Identity as maintained by the Identity Services.

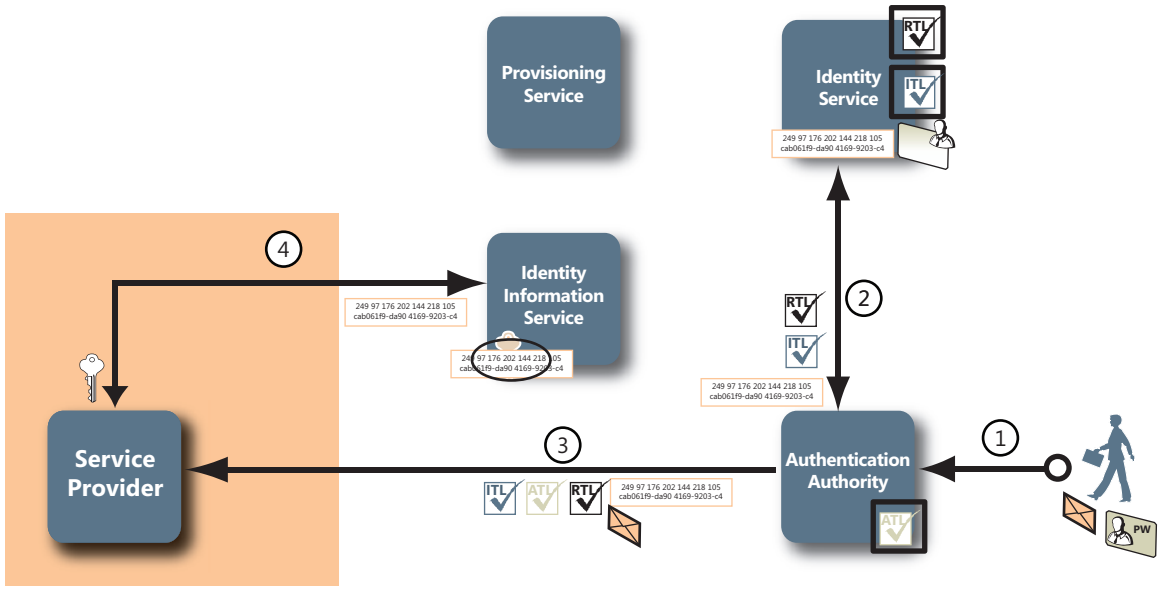
Let's consider a typical scenario for Authentication to illustrate the implementation of the Trust Model (see Figure 4, page 17).

(1) The Subject provides its Credentials to the Authentication Authority. (2) The Authentication Authority fetches the unique ID (a GUID in this example) and the ITL and RTL from the Identity Service. If needed, it may interrogate the Identity Service for more detailed information contained in the Trace object. The Authentication Authority determines the ATL and updates the Trace object to reflect the Authentication steps it has performed. (3) Subsequently, it propagates the service request to the Service Provider and embeds the Identity information and Session Trust object in the service call. (4) In this example, the Service Provider implements its own unique identifier (Domain Unique Identifier) for the identity and queries the Identity Information Service about the association of the unique identifier to the Domain Unique Identifier. The Service Provider can also fetch the Trace object from the Identity Information Service to get more detailed information if required.

Listing 2: Structure of the Trace object

```
Trace
    IdentificationProcess
    IdentificationStep (1-n)
            Policynumber (preferably an OID)
            ExecutedByWhom
                Name/IDno
                Institution
            DateTimeOfExecution
            ReferenceTo SourceDocuments
            AcceptanceOfIdentificationContract
    AuthenticationProcess
      AuthenticationStep (1-n)
            AuthenticationAuthority
            DateTimeOfAuthentication
            Credentials
            Medium/Channel
            Device
            Location
    ReputationHistory
      ReputationChange (1-n)
            PolicyNumber (preferably an OID)
            ExecutedByWhom
                InitiatedByWhom
                Name/IDno
            DateTimeOfExecution
            ReferenceTo SourceDocuments
```

Figure 4: Authentication



Conclusion

We started this by addressing the business and IT challenges. The ability to communicate Identity and Access Management information between parties is the key. Facilitating such communication requires quantifiable and verifiable Trust Levels. This applies to parties such as businesses within organizations, an organization with its partners, and also services in an SOA architecture.

Additionally, in order to meet the challenges, enable Access Control Policy enforcement at the to-be protected Resource at a level that is adequate for the situation at hand, tuned to the value/risk level of the transaction.

The architecture as developed — of which we discussed elements such as Session Trust object, Trace object and the mapping of the various Trust Levels to the value/risk levels of the business transactions — is capable of addressing these challenges from a technical perspective. However, it all boils down to the willingness of the parties involved to cooperate, to establish formal agreements for this cooperation, and to adhere to those agreements. But isn't that the main challenge in the whole Identity and Access Management domain?

Resources

International Telecommunication Union
ITU-T Recommendation X.509 (03/2000)

Web Services Security: SOAP Message Security 1.1,
OASIS Standard Specification, 1 February 2006

Web Services Security: SAML Token Profile 1,
OASIS Standard, 1 February 2006

Assertions and Protocols for the OASIS Security
Assertion Markup Language (SAML) V2.0,
OASIS Standard, 15 March 2005

Authentication Context for the OASIS Security
Assertion Markup Language (SAML) V2.0,
OASIS Standard, 15 March 2005

About the Authors

Gerrit J. van der Geest is an IT architect and program manager who has over 25 years experience in IT. Gerrit holds a master's degree in applied physics from the Eindhoven University of Technology in the Netherlands. He is cofounder of consultancy companies in the Netherlands and in South Africa. Prior to that, he held program management positions at Digital Equipment Corporation and Philips, where he was responsible for many international system integration programs.

Gerrit specializes in IAM, SOA, and infrastructure architecture and has been responsible for the development of IT strategies, domain, and solution architectures for large insurance and manufacturing organizations. Gerrit welcomes feedback at gerrit@navit.co.za.

Carmen de Ruijter Korver is a program manager with experience in IT infrastructure programs and architecture assignments. She worked for Compaq in the Netherlands, where she was responsible for the setup of a program management office and worked on many international IT infrastructure programs. Thereafter, she cofounded Navit (Pty) Ltd. in South Africa, where she specialized in the area of IAM with a focus on IAM migration strategies. Carmen is a PMI and PRINCE2 certified program manager.