



White Paper

Advanced Authentication

Introduction

In this paper:

Introduction 1

User Authentication 2

Device Authentication 3

Message Authentication 4

Advanced Authentication 5

Advanced Authentication is a key component of any Enterprise or Internet Security system, together with Authorisation, Administration, Encryption, Intrusion Detection, Anti-virus, Content Management and Firewalls.

At its simplest level authentication is a way of identifying the user of a system or the sender of a message. The authentication determines that the user is who they claim to be and thus is a vital component in Identity Management systems.

Identity Management systems combine processes for defining, creating, changing, deleting, authenticating, authorising and auditing users.

To understand the benefits of Advanced Authentication we must first understand authentication in general. In information technology systems there are three types of authentication:

1. User authentication
2. Device authentication
3. Message authentication

Here we take a look at the various forms of authentication, how they are applied and what services they provide.

User Authentication

User authentication involves confirming with a certain degree of confidence that the electronic form of the user's identity represented in the IT system corresponds to the real life identity of the user.

There are three factors of user authentication that may be used in combination to increase the level of confidence in the claimed identity of a user:

1. Something the user has
2. Something the user knows
3. Something the user is

Single Factor Authentication

The classic form of single factor authentication is user id and password. Here the user claims an identity by presenting a user id to the IT access control system and a secret password known only to the user and the IT access control system. The IT access control system checks the password for the claimed identity against its secure list of known identities and passwords.

If the user id and password pair, entered by the user, match the user id and password stored in the access control system then the user is judged to be authentic and given access to the system. This form of User Authentication while used extensively is relatively weak because the same password is used over and over again, giving many opportunities for it to be illicitly captured.

Another form of single factor authentication involves the use of an access control token, "something the user has", which can generate a sequence of passwords which change, say every 30 seconds. This is considered to be a stronger form of access control, because the password changes so frequently and there is no temptation to write it down. Also to access the system you must have access to the token and loss of the token is more obvious to the user than loss of a simple password. A stolen password may not be known to the user as they still have the password and can still gain access to the system.

Two Factor Authentication

Two factor authentication is considered to be stronger than single factor authentication. Two factor authentication usually involves using something you have, a token, and something you know, a Personal Identification Number (PIN). Two of the most widely used forms of two factor authentication are:

1. Automatic Teller Machine (ATM) or cashpoint machine card and PIN
2. Access control token and PIN

At an ATM the user puts their cashpoint card into the ATM and then the ATM requests the user to enter their PIN. The information held on the magnetic stripe of the card together with the PIN, encrypted in a secure block of data, is sent to the bank's central authentication system. Here the PIN entered by the user is compared with the PIN held on file against the user's account number and details. To maintain the confidentiality of the PIN at all times the PIN held on file is also encrypted and this comparison takes place inside the secure environment of a Hardware Security Module (HSM).

Two factor access control to a system usually involves using an access control token, to generate a dynamic password, and a PIN to activate the access control token. The access control token contains a secret cryptographic key. The user enters their user id to the access control system which then presents them with a random challenge. The user enters their PIN into their access control token, to activate the token, and then enters the random challenge, presented to them by the access control system. The access control token calculates a response to the random challenge, using its secret cryptographic key. The user presents this value to the access control system which checks that it is the correct response to the challenge using its copy of the secret key held in the token. The access control system has a record of all tokens issued to the users and a copy of the secret keys held in them. These values are stored securely encrypted on file. In order to check the validity of a response the access control system has to be able to perform the same calculation as the tokens, using the secret keys. To maintain the integrity and security of the system these calculations are usually performed inside an HSM. This method of User Authentication is strong because the challenge changes every time, making the capture of a challenge / response worthless.

An alternative form of two factor authentication involves using a token and a biometric, "Something the user is". Here the access control system takes a biometric reading from the user, such as a fingerprint, iris scan or voice print and compares the reading with a previously recorded value. This recorded value can be either stored on the token or on a central database. Once the biometric value has been read then it can be used in the same way as a PIN.



Three Factor Authentication

Three factor authentication is considered to be the strongest form of user authentication available. This involves using an access control token, such as a smart card, a PIN to access the smart card and a biometric value held in a central database. The card is entered into a reader, the PIN is entered via a special PIN pad or keyboard, the biometric is read and encrypted under a cryptographic key held on the smart card.

The user id, read from the smart card, together with the encrypted biometric are sent to the central access control system where the biometric can be decrypted and compared with the value on the central access control database. To maintain the integrity and security of the system the cryptographic calculations and validation of the biometric are usually performed inside an HSM. Note here that the user PIN is not sent to the central access control system, but is checked locally by the smart card.

Device Authentication

Sometime it is necessary to check the authenticity of the terminal which is being used by the user. For instance a bank's host system will check that the message it has received has come from one of its own ATMs or one of its Electronic Point of Sale (EPoS) terminals. This is usually achieved in one of two ways:

1. Master/Session key cryptography
2. Transaction key cryptography

Master/Session Key Cryptography

In master/session key cryptography the ATM is initialised with a Terminal Master Key which is then used to establish a session key between the ATM and the bank's host system on a regular basis, say once a day. When the bank host computer receives a transaction from the ATM it can be reasonably sure that the message came from that ATM if the message was secured using the session key which the host computer has associated with the ATM. To maintain the integrity and security of the system these keys are only used inside an HSM. Changing the session key frequently reduces the chance of "brute force" (exhaustive key searches) being successful.

Transaction Key Cryptography

In transaction key cryptography the EPoS terminal is initialised with a transaction key value. This value is then updated after every transaction so that a new transaction key is used to secure each transaction between the terminal and the bank's host computer. Because the bank's host computer also knows the mechanism for changing the key after each transaction it can keep in step with the terminal and will only accept transactions secured using the current and correct transaction key value. Again, to maintain the integrity and security of the system the transaction keys are only ever generated and used inside an HSM. This type of scheme often employs additional mechanisms to prevent tracking forwards and backwards should a single key ever be compromised. Thus stealing a terminal is of little value.

Message Authentication

There are two types of IT communication systems:

1. Session based communications
2. Message based communications



Session Based Communications

Session based communications involve establishing an agreed set of communications parameters, a context, which is maintained for the duration of the session. The session usually involves data flowing backwards and forwards between the two communicating devices, e.g. client and server, web browser and web server. If the communication is to be secure then various security parameters, such as cryptographic keys, are also agreed at the start of the session and maintained as part of the session context. Once the session is over the context is lost and the cryptographic session keys are deleted.

If a user is to be involved in the session then it may be necessary for the user to logon and be authenticated in order to establish the session. This user logon and user authentication can be achieved using any one of the methods described above in the section on User Authentication.

Message Based Communications

Message based communications do not require a session to be established or a user logon. Each message is a complete package of information and the recipient computer decides whether to accept and process the message or reject it based on its construction and content. In order to take this decision the receiving computer usually needs to know who sent the message and has the message been accidentally or purposely modified since it left the sender. This requirement is known as message integrity or message authentication. There are two ways to ensure the integrity of a message:

1. Message authentication codes
2. Digital signatures

Message Authentication Codes

Message authentication codes are cryptographic checksums generated using a symmetric key. The message authentication code (MAC) is appended to the cleartext message – it does not provide message confidentiality. The recipient of the message can re-calculate a MAC for the message they received and compare it with the MAC received with the message. If the two values are the same then the recipient can be confident that the message they received is exactly the same as the message that was originally sent.

If only the sender and the recipient know the cryptographic key used to generate the original MAC then the recipient can also be confident of the identity of the sender. That is assuming that the key was originally distributed securely, to the correct identity and that person or system has stored and used the key securely. This is the Key Management problem which is a feature of any cryptographic system. Key management covers the secure creation, distribution, storage, use, replacement and destruction of cryptographic key material.

Digital Signatures

Digital signatures are another form of cryptographic checksum generated using Public Key cryptography. Unlike symmetric key cryptography where the sender and recipient share the same key, in public key cryptography the sender and recipient have different, but related, cryptographic keys. This is why it is also known as asymmetric key cryptography. The sender has a private key, which only they know, and the recipient has the corresponding public key, which in fact anyone can know, hence the name Public Key cryptography.

The sender of the message generates a compressed form of the message, known as a hash, which is in fact a cleartext checksum not involving a key. This hash value is then encrypted using the sender's private key the result being the digital signature for that user of the message. The digital signature is appended to the cleartext message – again it does not provide message confidentiality. The recipient of the message cannot calculate the digital signature because they do not have a copy of the sender's private key.



However, they can decrypt the digital signature to reveal the hash value calculated by the sender. Now they can re-compute the hash value on the received message and compare it with the hash value retrieved from the digital signature. If the two values are the same then the recipient can be confident that the message they received is exactly the same as the message that was originally sent. Because the sender should be the only person or system to have access to the private key then the recipient can be also confident in the identity of the sender. Again this confidence is dependent on a robust key management scheme supporting the system and this is normally provided in the form of a Public Key Infrastructure (PKI).

Advanced Authentication

The term Advanced Authentication can apply to any or all of the three forms of authentication:

1. User authentication
2. Device authentication
3. Message authentication

For it to be an Advanced Authentication it must use cryptographic keys, supported by a robust key management system, and tamper resistant hardware security modules. The authentication parameters generated at the user-end can be calculated using secret or public key cryptography, with keys stored on hand-held tokens, dongles, smart cards, soft tokens or cryptographic co-processors. Advanced Authentication, managed through a single platform, which can apply an appropriate level of security, depending on the risk profile for each application provides a standard way of supporting the variety of hardware and software based authentication devices.

In many identity management systems there is a move to Advanced Authentication to support multi-factor authentication providing increased levels of trust and lower levels of risk. Advanced Authentication servers are helping to ease the difficulties of moving existing authentication applications towards more integrated identity management systems.

In response to Homeland security initiatives there is a need for stronger authentication of individuals and a tighter integration of both physical and logical access control. As these physical and logical security worlds combine Advanced Authentication systems will play a key role as a single point of user authentication.

With the increase of Internet and mobile commerce transactions and the associated increase in fraud, it is becoming crucial that the financial institutions, service operators and merchants are able to authenticate not only the device but also, more importantly, the actual user. However, these systems are characterised by a proliferation of user interface devices - personal computers, mobile phones, interactive television, a variety of mobile terminals and service kiosks. The user authentication devices are equally diverse and the ability to manage this complexity through a single Advanced Authentication platform will provide simplified integration, consistency of security and reduced operational cost.

THALES

EUROPE, MIDDLE EAST, AFRICA THALES e-SECURITY LTD.

Meadow View House
Long Crendon, Aylesbury
Buckinghamshire, HP18 9EG, UK
Tel: +44 (0)1844 201800
Fax: +44 (0)1844 208550
e-mail: [emea.sales@thales-
ecurity.com](mailto:emea.sales@thales-
ecurity.com)

AMERICAS

THALES e-SECURITY, INC.

2200 N. Commerce Parkway
Suite 200
Weston, Florida 33326, USA
Tel: +1 888 744 4976
or: +1 954 888 6200
Fax: +1 954 888 6211
e-mail: [americas.sales@thales-
ecurity.com](mailto:americas.sales@thales-
ecurity.com)

ASIA PACIFIC

THALES e-SECURITY (ASIA) LTD.

Asia Pacific
Units 2205-06, 22/F Vicwood Plaza,
199 Des Voeux Road
Central, Hong Kong, PRC
Tel: +852 2815 8633
Fax: +852 2815 8141
e-mail: [asia.sales@thales-
ecurity.com](mailto:asia.sales@thales-
ecurity.com)