INF3510 Information Security
University of Oslo
Spring 2011

Lecture 7

Authentication

Audun Jøsang

Outline

- Concepts related to authentication
- User Authentication
  - Knowledge-Based Authentication
    - Passwords
  - ID-Based Authentication
    - Biometrics
  - Object-Based Authentication
    - Tokens
- Message Authentication
  - Usability of cryptographic message authentication
  - Strength of electronic signatures

Authentication according to X.800

Peer-entity authentication

- *"The corroboration that a peer entity in an association is the one claimed."*

same as:

User/entity Authentication

Data origin authentication

- *"The corroboration that the source of data received is as claimed."*

same as:

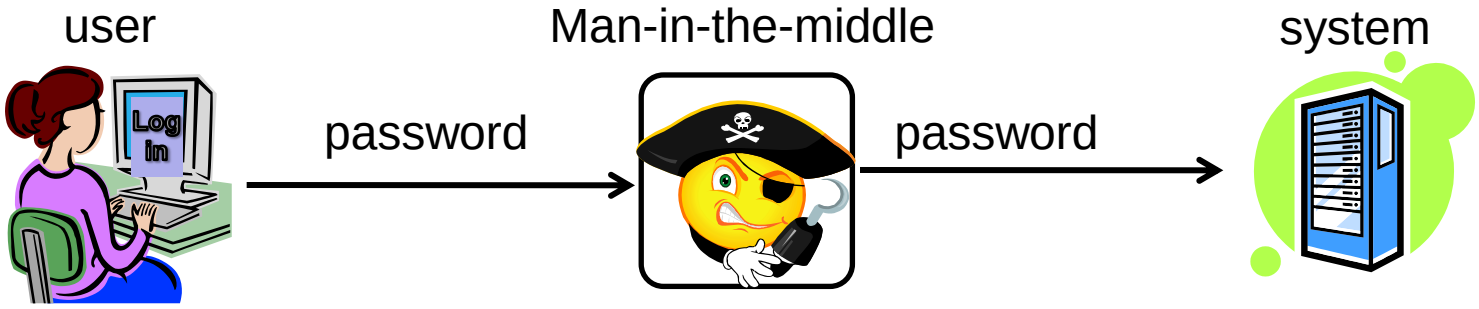
Message Authentication

User / Entity Authentication

- **User authentication** means that a system verifies the user's claim of holding a specific identity
  1. The user presents an identity (e.g. logon id)
  2. The user produces an identity proof (e.g. password)
- **Entity authentication** means that a user or system verifies another entity's claim of holding a specific identity.
  1. The entity presents an identity (e.g. e domain name)
  2. The entity produces an identity proof (e.g. Challenge-response exchange)

User / Entity Authentication

- Applies to the start of a session (association) between a user/entity and a system.
- Assumes e.g. a user operating a terminal
- Does not guarantee that received messages originate from the user/entity or terminal.
  - Somebody else can take over the terminal or session
  - There can be a man-in-the-middle attack



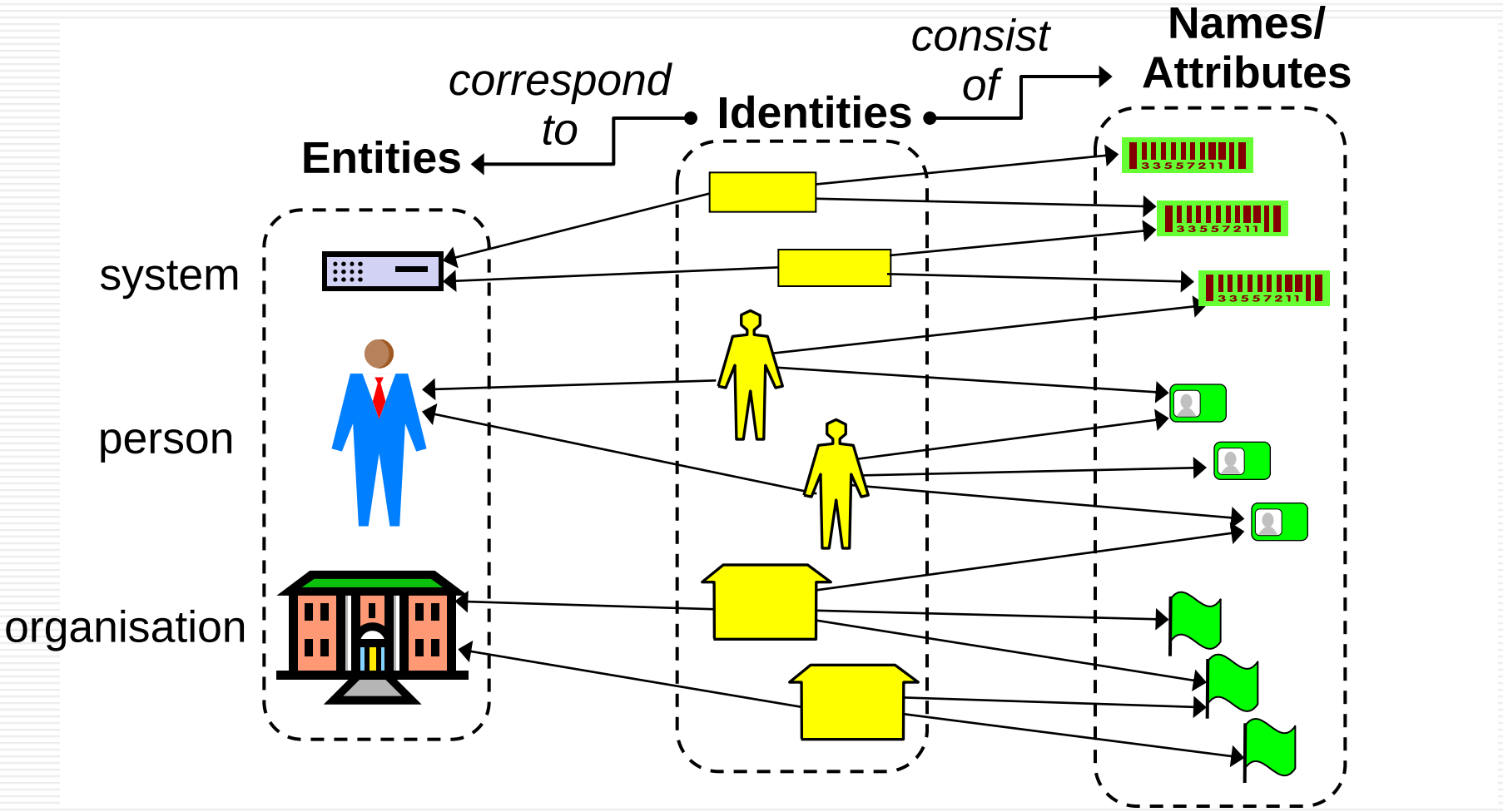
Data Origin / Message Authentication

- Provides evidence that the message or data was sent by a user or entity with a specific identity
- Strong message authentication requires cryptographic protection
  - Encryption, MAC, digital signature
- Weak message authentication only needs some form of electronic evidence , e.g.:
  - Sender address in header of email
  - Sender phone number of SMS message

Identity

- Etymology of *“identity”* simply expresses that the entity is *“the same one as last time”.*
- “First-time” authentication not meaningful
  - “First time” is the registration of new identity
- Authentication normally requires a first time registration of identity (with name)
- Registration can require pre-authentication
- Names can be difficult to interpret:
  - What about the name “apple” which could be: “apple123@hotmail.com”, www.applecorp.com, “www.apple.com”, “apple computers”, ”apple records” ?

The Concept of Identity



Concepts related to identity

- Entity
  - A person, organisation, agent, system, etc.
- Identity
  - A set of names / attributes of entity in a specific domain
  - An entity may have multiple identities in one domain
- Digital identity
  - Digital representation of names / attributes in a way that is suitable for processing by computers
- Names and attributes of entity
    - Can be unique or ambiguous within a domain
    - Transient or permanent, self defined or by authority, interpretation by humans and/or computers, etc

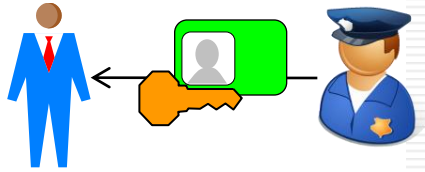
User/Entity Authentication

Stages of User Authentication

Registration phase (only once)

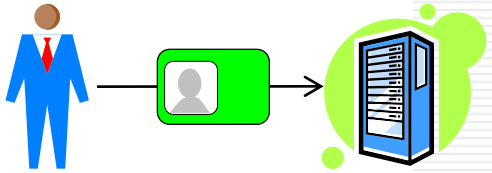
1. Registration
   - User contacts ID-provider, possibly with documentation (aka. pre-authentication)

2. Provisioning
   - ID-provider registers unique name and issues credential

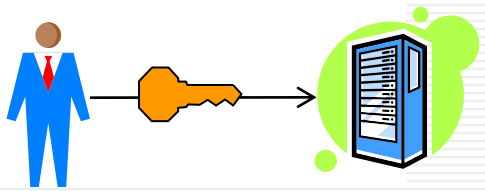


Authentication phase (multiple times)

3. Identification
   - User presents the unique name to select his identity



4. Verification of identity
   - Proves Id with credential



Types of entity authentication:

- Person authentication:
  - Verify correctness of person's claimed identity
  - Identity may be recognised as
    - name: e.g. Mr. Apple
    - role: e.g. secret spy
    - attribute: older than 18 years of age
- Machine / system authentication
  - Verify system identifier
- Organisation authentication
  - Verify attribute of org., or its authorized representative
  - May require person authentication

Authentication Credentials: Overview

- The ‘thing’ used to perform authentication is called a credential
  - May also be referred to as a “token” or “authenticator”
  - e.g. reusable passwords, PIN, biometrics, smart cards, certificates, cryptographic keys, OTP hardware tokens.
- Categories include:
  - Knowledge-Based (Something you know)
  - Object-Based (Something you have)
  - ID-Based (Something you are)
  - Location-based (Somewhere you are)
  - Plus combinations of the above

Knowledge-Based Authentication

Something you know: Passwords

Authentication: Reusable passwords

- Passwords are a simple and most-often-used authenticator.
  - Something the user knows
- Problems:
  - Easy to share (intentionally or not) and forget.
  - Often easy to guess
  - Can be written down
  - Do not provide non-repudiation.

Strategies for strong passwords

- User education
- Computer-generated passwords
- Proactive password checking
- Reactive password checking

Passwords: User education

- Part of the organisation's security policy.
- Users are told the importance of choosing 'strong' passwords.
- It is unlikely to be effective in most organisations, particularly where there is:
  - a large user population or
  - a high turnover of users.
- Some users simply ignore guidelines or are poor at selecting a 'strong' password.
  - Likely to choose passwords that are too short or too easy to guess.

RockYou Hack

- 32 million passwords stolen from RockYou in December 2009
- Posted on the Internet
- Contains accounts and passwords for websites
  - MySpace, Yahoo, Hotmail
- Analyzed by Imperva.com
  - 1% uses 123456
  - 20% uses password from set of 5000 different passwords

MOST POPULAR PASSWORDS

Nearly one million RockYou users chose these passwords to protect their accounts.

1.	**123456**	17.	**michael**
2.	**12345**	18.	**ashley**
3.	**123456789**	19.	**654321**
4.	**password**	20.	**qwerty**
5.	**iloveyou**	21.	**iloveu**
6.	**princess**	22.	**michelle**
7.	**rockyou**	23.	**111111**
8.	**1234567**	24.	**0**
9.	**12345678**	25.	**tigger**
10.	**abc123**	26.	**password1**
11.	**nicole**	27.	**sunshine**
12.	**daniel**	28.	**chocolate**
13.	**babygirl**	29.	**anthony**
14.	**monkey**	30.	**angel**
15.	**jessica**	31.	**FRIENDS**
16.	**lovely**	32.	**soccer**

Source: Imperva

Passwords strategies

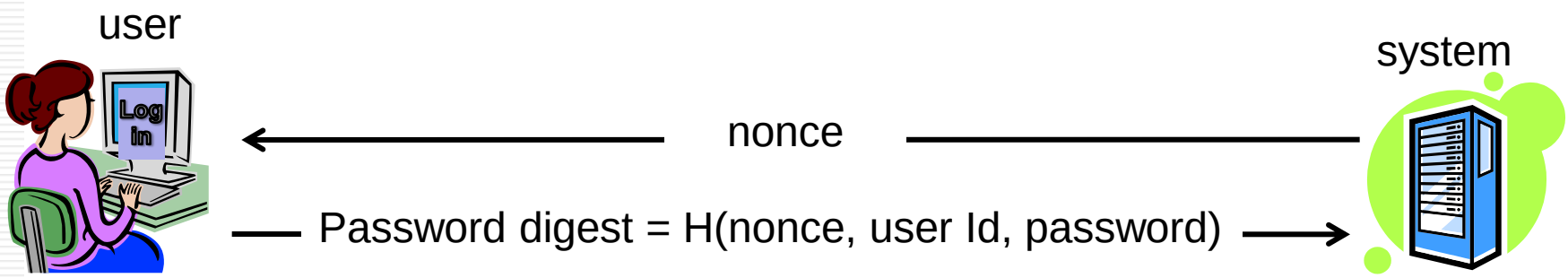
- Computer generated passwords
  - Users unable to remember and write random passwds
  - FIPS PUB 181 http://www.itl.nist.gov/fipspubs/fip181.htm specified automated pronounceable passwd generator
- Proactive password checking
  - user selects a potential password which is tested
  - Balance is required for acceptable and non-acceptable
- Reactive password checking
  - System administrator periodically runs a password cracking tool (those available to attackers) and seeks those passwords that are easy to recover.

Authentication: Problems with using passwords in the clear

- A password sent “in clear” can be captured during transmission, so an attacker may reuse it.
- An attacker setting up a fake server can get the password from the user
  - E.g. phishing attack.
- Solutions to these problems include:
  - Password encryption
  - One-time passwords (described under token authent.)
  - Challenge-response protocols
  - Server authentication

Digest Authentication
A simple challenge-response protocol

- attempts to overcome the shortcomings of Basic Authentication
- WWW-Authenticate = Digest realm="defaultRealm" nonce="Server SpecificString"
- see RFC 2069 for description of nonce, each nonce is different
- the nonce is used in the browser in a 1-way function (SHA-1….) to produce a password digest of user Id and password
- the transmitted password digest is valid only once



ID-Based Authentication

Something you are: Biometrics

Biometrics: Overview

- Why use it?
  - convenient as it can not be lost or forgotten
  - provides for positive authentication
    - Difficult to copy, share, and distribute
    - Passwords and token can be loaned to others
    - Require the person being authenticated to be present at the time and point of authentication.
  - increasingly socially acceptable
  - becoming less expensive
  - considered very effective as part of a two-factor authentication scheme.
  - can also be used for identification

Biometrics: Overview

- What is it?
  - Automated methods of verifying or recognizing a person based upon a physiological characteristics.
- Biometric examples:
  - fingerprint
  - facial recognition
  - eye retina/iris scanning
  - hand geometry
  - written signature
  - voice print
  - keystroke dynamics

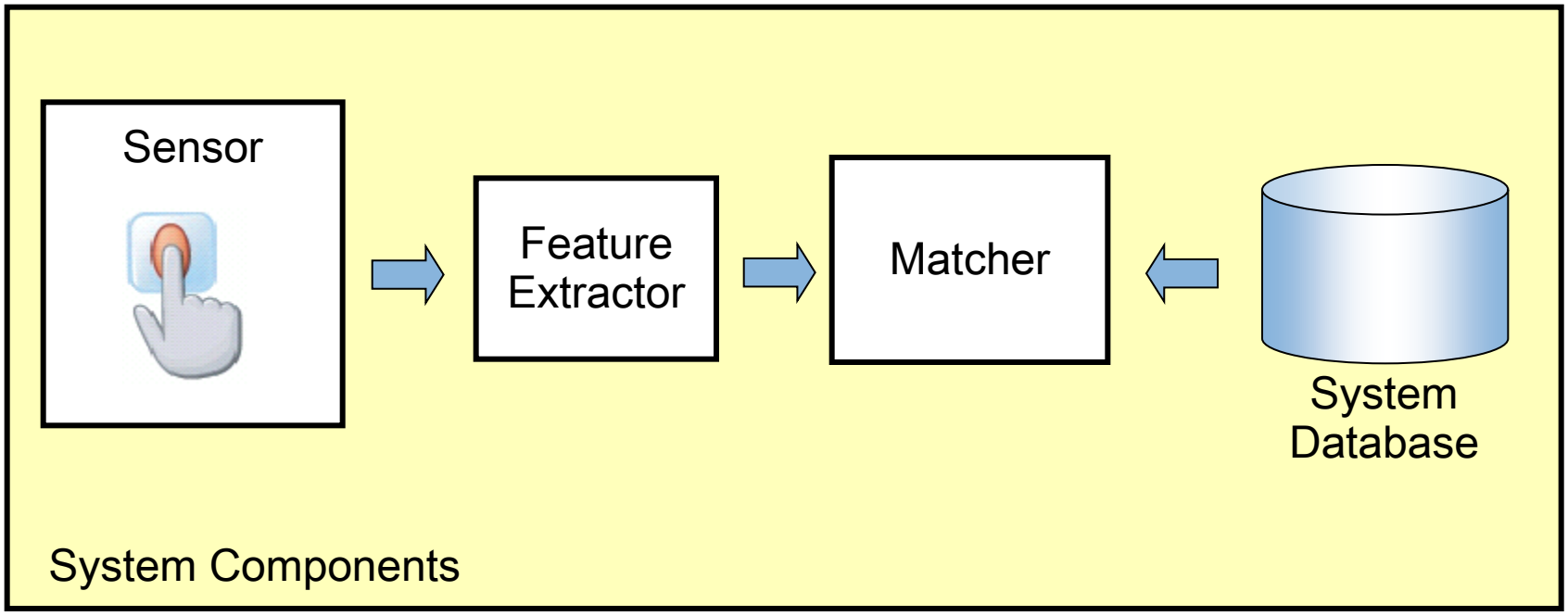
Biometrics: Characteristic requirements

- **Universality**:
  each person should have the characteristic;
- **Distinctiveness**:
  any two persons should be sufficiently different in terms of the characteristic;
- **Permanence**:
  the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time;
- **Collectability**:
  the characteristic can be measured quantitatively.

Biometrics: Practical considerations

- Performance:
  - the achievable recognition accuracy and speed,
  - the resources required to achieve the desired recognition accuracy and speed,
  - the operational and environmental factors that affect the accuracy and speed;
- Acceptability:
  - the extent to which people are willing to accept the use of a particular biometric identifier (characteristic)
- Circumvention:
  - how easily can the system be fooled

Biometrics: System components



Biometrics: System components

- Sensor module: captures the biometric signal of an individual.
  - An example is a fingerprint sensor that images the ridge and valley structure of a user's finger.
- Feature extraction module: processes the acquired biometric signal to extract a set of salient or discriminatory features.
  - For example, the position and orientation of minutiae points (local ridge and valley singularities) in a fingerprint image are extracted in the feature extraction module of a fingerprint-based biometric system.

Biometrics: System components

- Matcher module: features captured during recognition are compared against the stored templates to generate matching scores.
  - For example, in the matching module of a fingerprint-based biometric system, the number of matching minutiae between the input and the template fingerprint images is determined and a matching score is reported. The matcher module also encapsulates a decision making module, in which a user's claimed identity is confirmed (verification) or a user's identity is established (identification) based on the matching score.

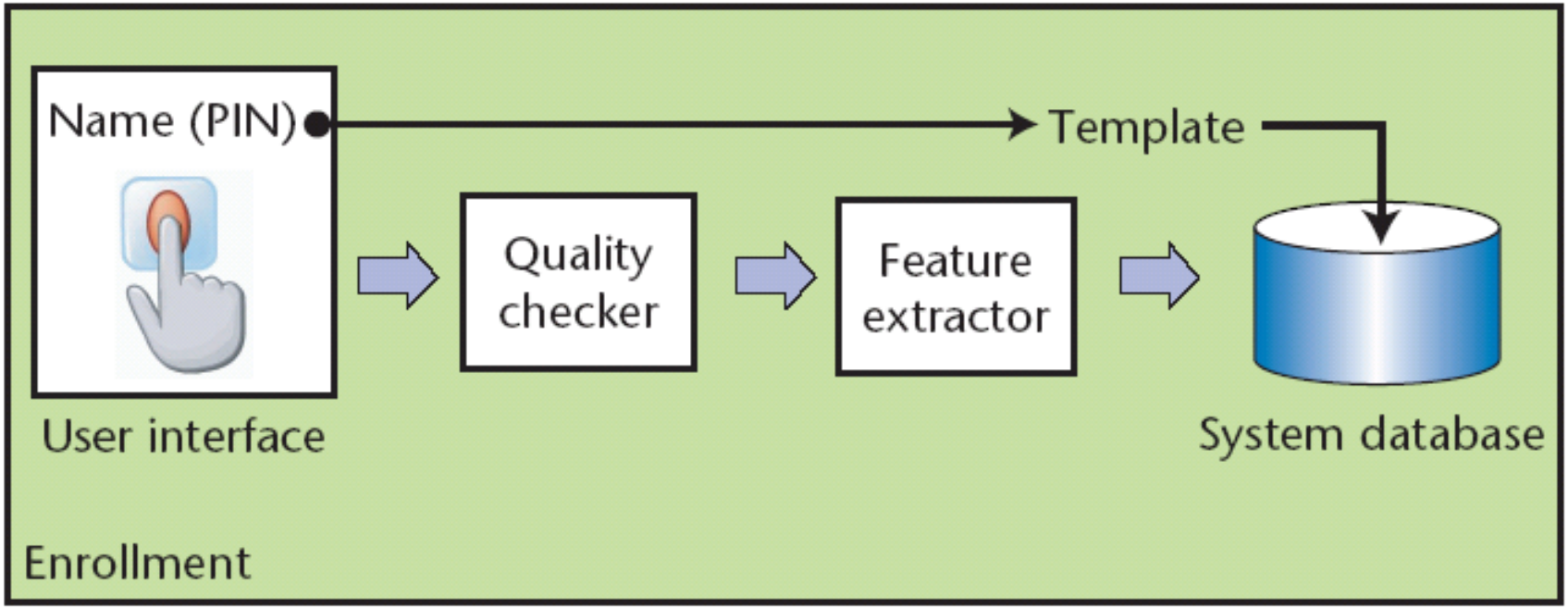
Biometrics: System components

- System database module: used by the biometric system to store the biometric templates of the enrolled users.
  - The enrolment module is responsible for enrolling individuals into the biometric system database.
  - During the enrolment phase, the biometric characteristic of an individual is first scanned by a biometric reader to produce a digital representation (feature values) of the characteristic.
  - The data capture during the enrolment process may or may not be supervised by a human depending on the application.

Biometrics: Modes of operation

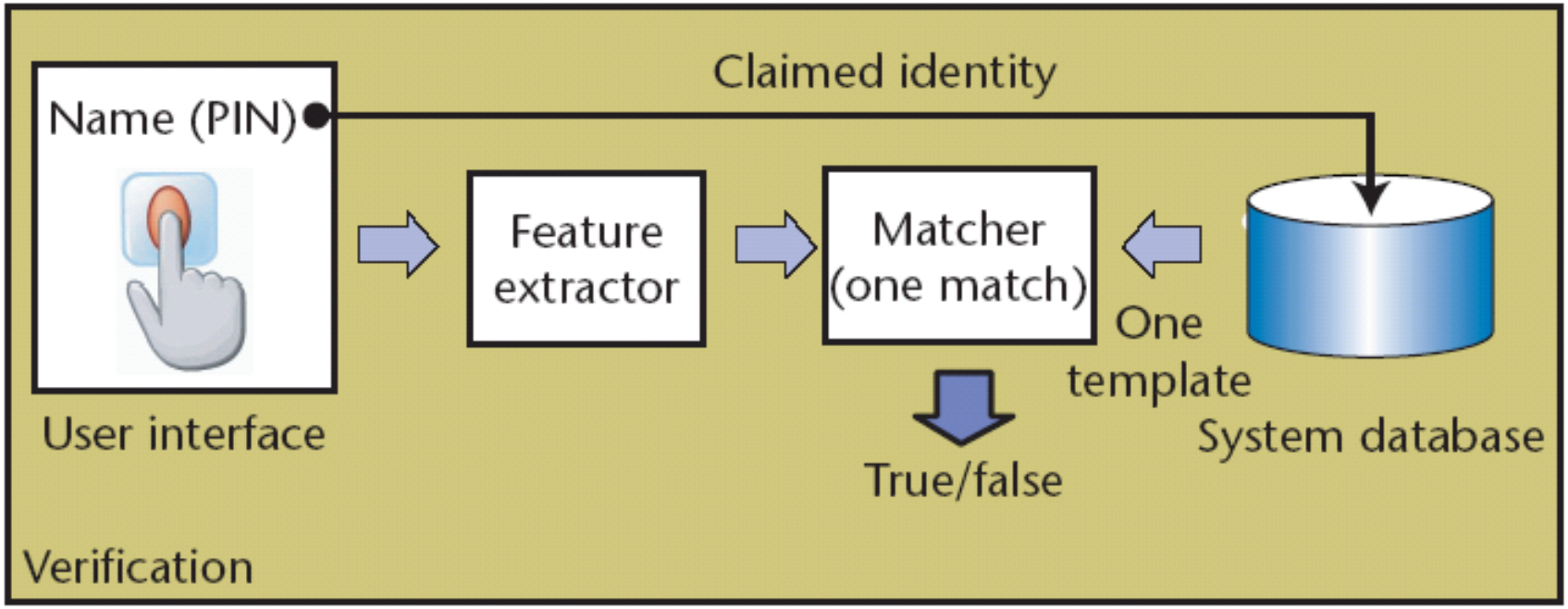
- Enrolment:
  - analog capture of the user's biometric attribute.
  - processing of this captured data to develop a template of the user's attribute which is stored for later use.
- Identification (1-to-many):
  - capture of a new biometric sample.
  - search the database of stored templates for a match based solely on the biometric.
- Verification of claimed identity (1-to-1):
  - capture of a new biometric sample.
  - comparison of the new sample with that of the user's stored template.

Biometrics: Enrolment



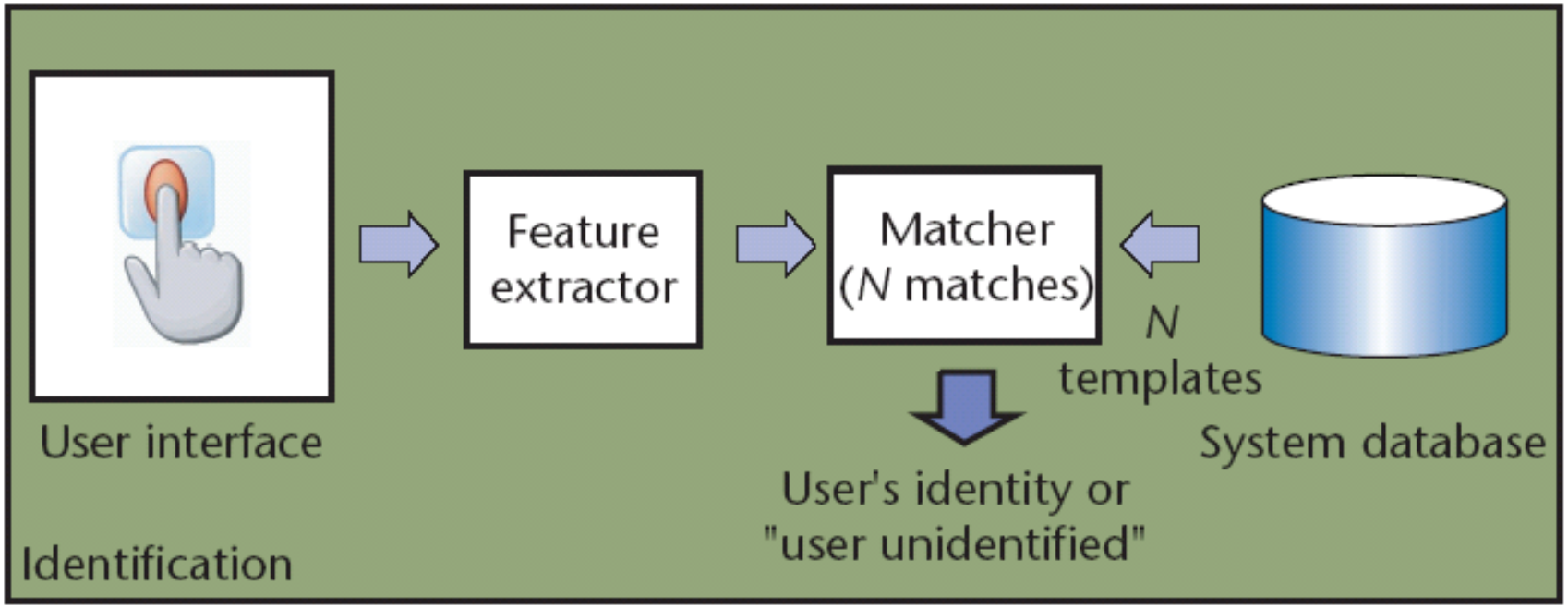
Biometric Recognition: Security and Privacy Concerns

Biometrics: Verification



Biometric Recognition: Security and Privacy Concerns

Biometrics: Identification



Biometric Recognition: Security and Privacy Concerns

Biometrics Safety

- Biometric authentication can be safety risk
  - Attackers might want to “steal” body parts
  - Subjects can be put under duress to produce biometric authenticator
- Necessary to consider the physical environment where biometric authentication takes place.

Car thieves chopped off part of the driver’s left index finger to start S-Class Mercedes Benz equipped with fingerprint key. Malaysia, March 2005
(NST picture by Mohd Said Samad)

Evaluating Biometrics: System Errors

- Two samples of the same biometric characteristic from the same person (e.g., two impressions of a user's right index finger) are not exactly the same due to
  - imperfect imaging conditions (e.g. sensor noise and dry fingers),
  - changes in the user's physiological or behavioral characteristics (e.g. cuts and bruises on the finger),
  - ambient conditions (e.g. temperature and humidity) and
  - user's interaction with the sensor (e.g. finger placement).

Evaluating Biometrics: System Errors

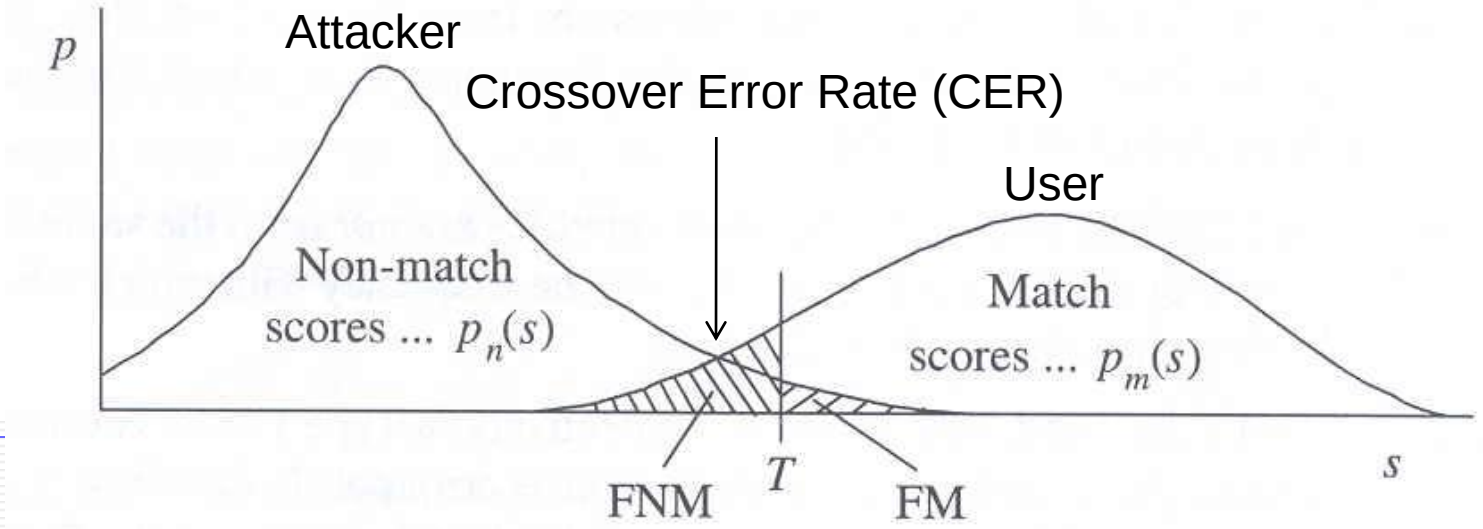
- Features captured during recognition are compared against the stored template
- The higher the score, the more certain the system is that the two biometric measurements come from the same person.
- The system decision is tuned by threshold *T*:
  - pairs of biometric samples generating scores higher than or equal to *T* are inferred as mate pairs (same person)
  - pairs of biometric samples generating scores lower than *T* are inferred as non-mate pairs (different person)

Evaluating Biometrics: System Errors

- A biometric verification system makes two types of errors:
  - False positive: Mistaking biometric measurements from two different persons to be from the same person (called false match), and
  - False negative: Mistaking two biometric measurements from the same person to be from two different persons (called false non-match).
- There is a trade-off between false match rate (FMR) and false non-match rate (FNMR) in every biometric system.

Evaluating Biometrics: System Errors

- FMR and FNMR are functions of the threshold *T*.
  - If *T* is decreased to make the system more tolerant to input variations and noise, then FMR increases.
  - On the other hand, if *T* is raised to make the system more secure, then FNMR increases accordingly.
- Ex. score distributions of attacker and user subject:



Object-Based Authentication

Something you have: Tokens

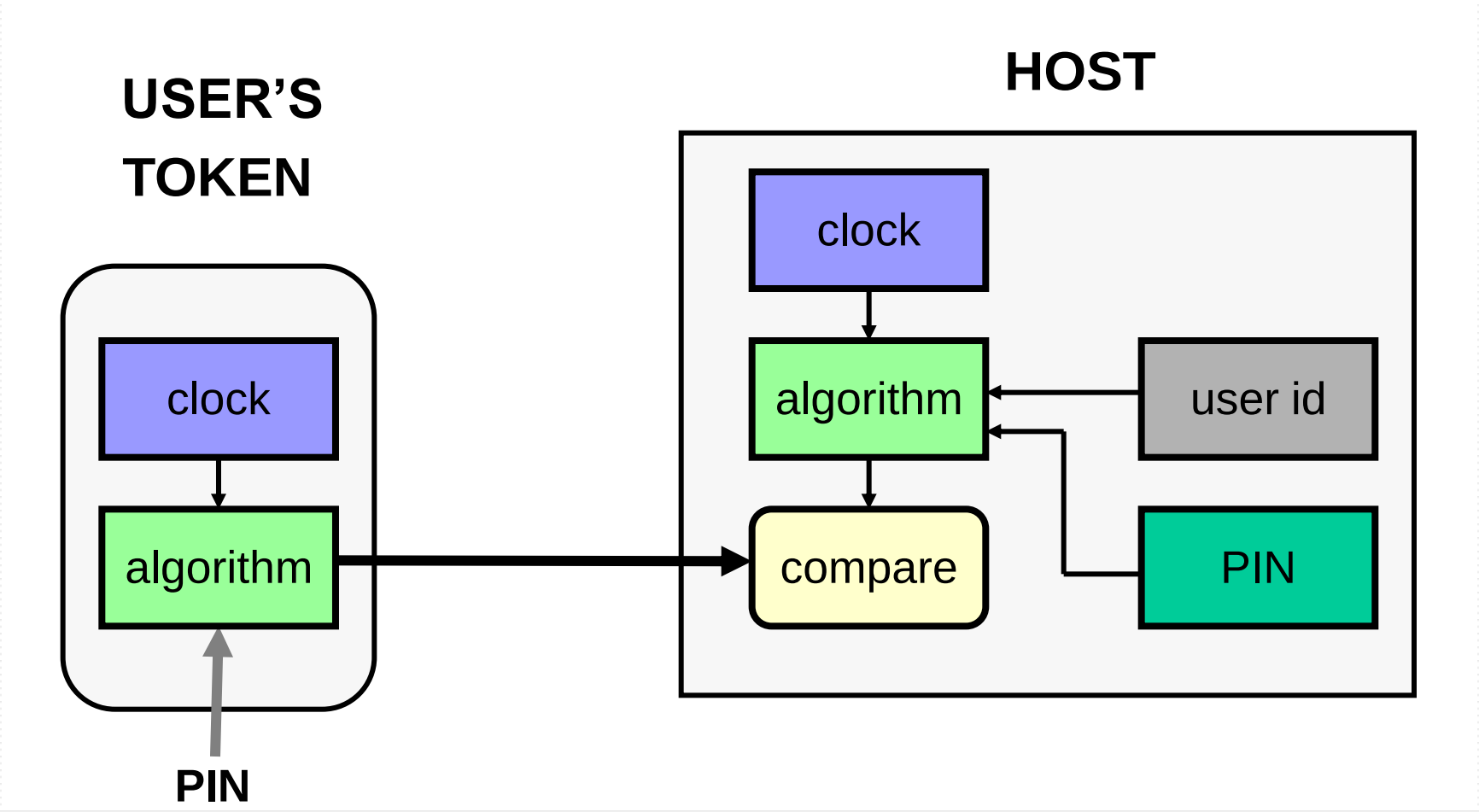
Synchronised OTP (One-Time-Password) Generator

- Using a password only once significantly strengthens the security of the user authentication process.
- Synchronized password generators produce the same sequence of random passwords in a token and at the host system.
  - Is this ‘something you know’ or ‘something you have’?
- There are two general methods:
  - Clock-based tokens
  - Counter-based tokens

Clock-based OTP Tokens: Operation

- Token displays time-dependent code on display
  - User copies code from token to terminal to log in
- Possession of the token is necessary to know the correct value for the current time
- Each code computed for specific time window
- Codes from adjacent time windows are accepted
- Clocks must be synchronised
- Example: BankID and SecurID

Clock-based OTP Tokens: Operation



Clock-based OTP Tokens: RSA SecurID tokens and BankID tokens

RSA SecurID SD600

RSA SecurID SID700

RSA SecurID SD200

BlackBerry with
RSA SecurID software token

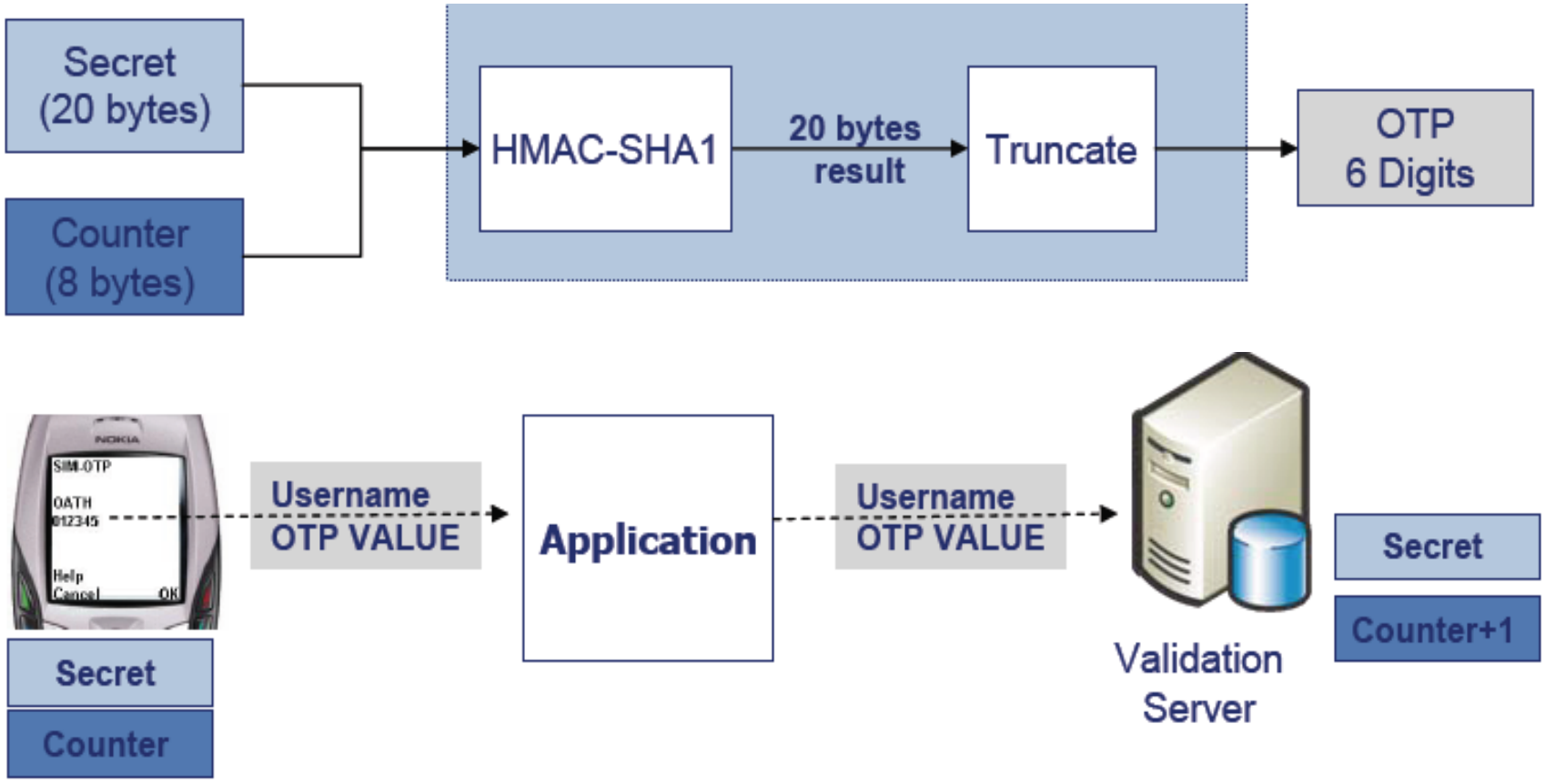
BankID OTP
calculator with PIN

BankID OTP
calculator without PIN

Counter-based OTP Tokens: Overview

- Counter-based tokens generate a ‘password’ result value as a function of an internal counter and other internal data, without external inputs.
- HOTP is a HMAC-Based One-Time Password Algorithm described in RFC 4226 (Dec 2005)
  http://www.rfc-archive.org/getrfc.php?rfc=4226
  - Tokens that do not support any numeric input
  - The value displayed on the token is designed to be easily read and entered by the user.
  - Example: Axalto Protiva

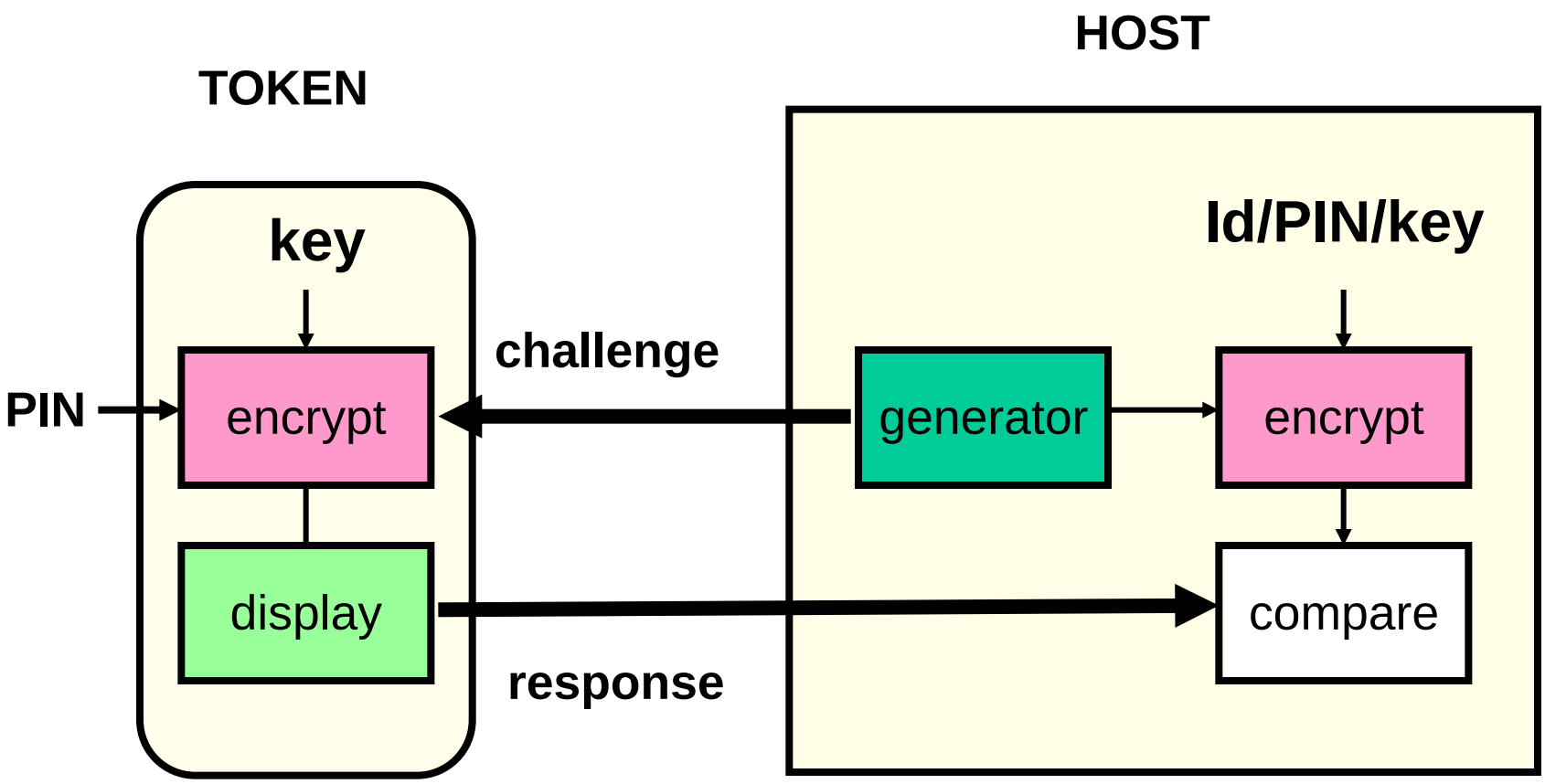
Counter-based OTP Tokens: HOTP



Token-based User Authentication: Challenge Response Systems

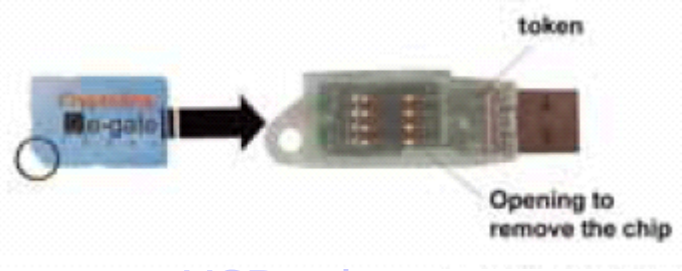
- A challenge is sent in response to access request
  - A legitimate user can respond to the challenge by performing a task which requires use of information only available to the user (and possibly the host)
- User sends the response to the host
  - Access is approved if response is as expected by host.
- Advantage: Since the challenge will be different each time, the response will be too – the dialogue can not be captured and used at a later time
- Could use symmetric or asymmetric crypto

Token-based User authentication Challenge Response Systems

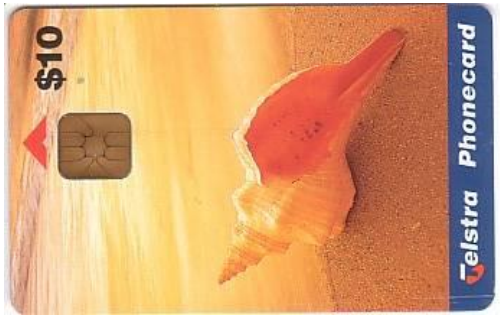


Symmetric Case

ICC with Contacts: Types



USB token

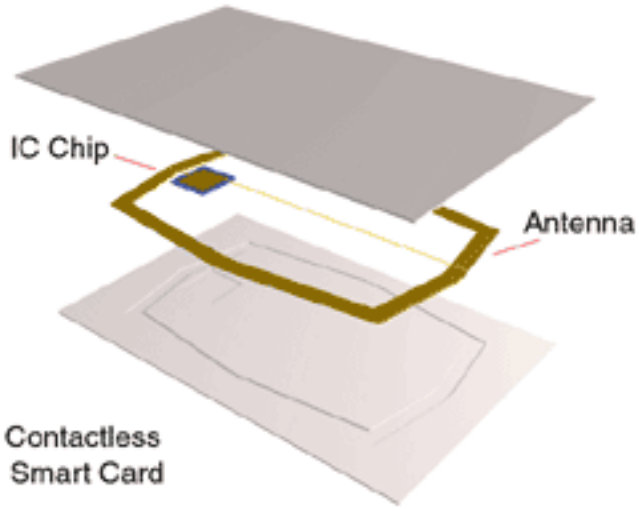


Java card

http://www.cryptoflex.com/

Contactless Cards: Overview

- Contactless IC consists of a chip and an antenna.
  - Does not need to come into contact with the machine (RF) reader.
  - When not within the range of a machine (RF) reader it is not powered and so remains inactive.
- Suitable for use in hot, dirty, damp, cold, foggy environments

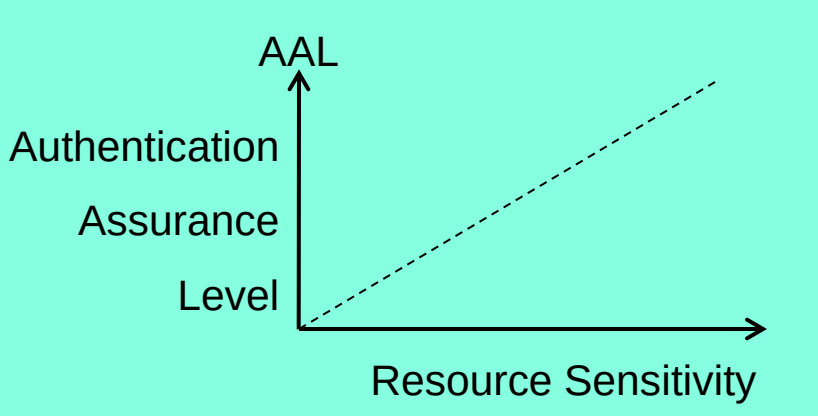


Authentication: Multi-factor

- Multi-factor authentication aims to combine two or more authentication techniques in order to provide stronger authentication assurance.
- Two-factor authentication is typically based on something a user knows (factor one) plus something the user has (factor two).
  - Usually this involves combining the use of a password and a token
  - Example: BankID OTP token and PIN

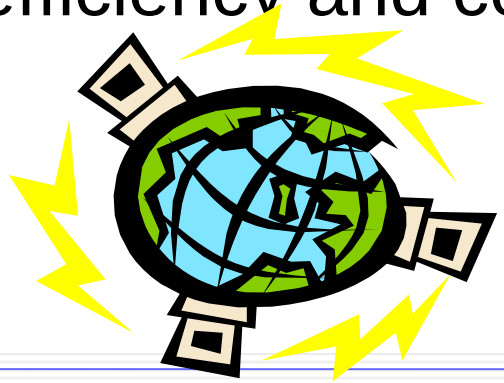
Authentication Assurance

- Resources have different sensitivity levels
  - Higher sensitivity requires stronger user authentication
- Authentication has a cost
  - Stronger user authentication costs more
- The authentication assurance level should match the sensitivity level



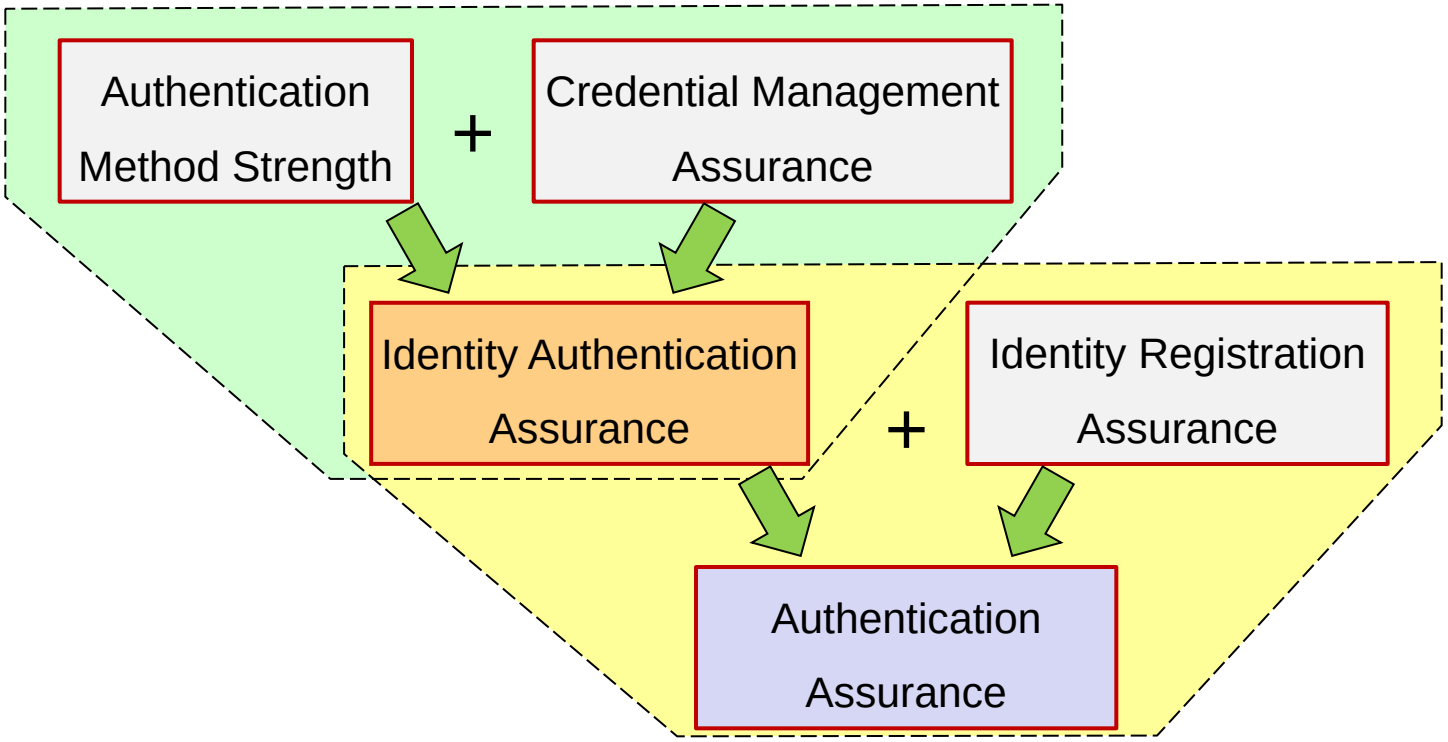
Why authentication frameworks?

- Trust in identity is a requirement for e-business.
- Authentication assurance produces identity trust.
- Authentication depends on technology, policy, standards, practice, behaviour and regulation.
- Consistency of approach allows cross-national and cross-organisational schemes that enable convenience, efficiency and cost savings.



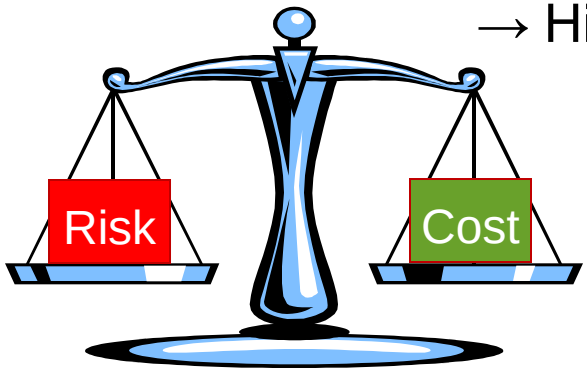
Authentication Assurance

- Do we have the correct party at the other end of the line?
- Authentication assurance through the combination of:



Authentication Assurance Requirement

- Application sensitivity
  - Higher Sensitivity
  - → Higher Risk
- Authentication cost
  - Stronger Authentication
  - → Higher Cost



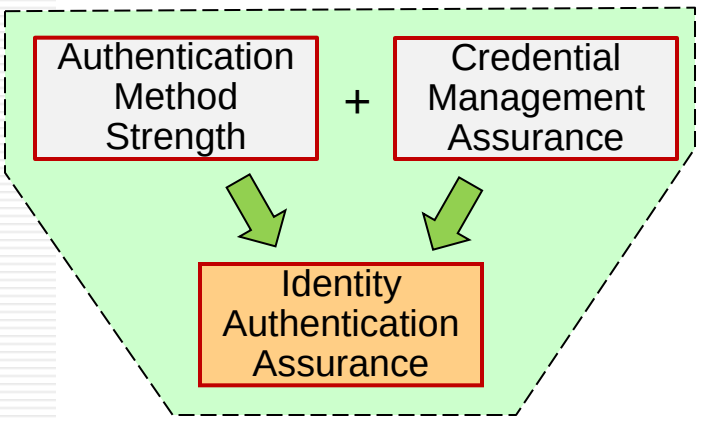
- Authentication assurance should reflect application sensitivity.
- Cost of authentication must balance risk of authentication error.

AAL: Authentication Assurance Levels

No Assurance	Minimal Assurance	Low Assurance	Moderate Assurance	High Assurance
Level 0	Level 1	Level 2	Level 3	Level 4
No registration of identity required	Minimal confidence in the identity assertion	Low confidence in the identity assertion	Moderate confidence in the identity assertion	High confidence in the identity assertion

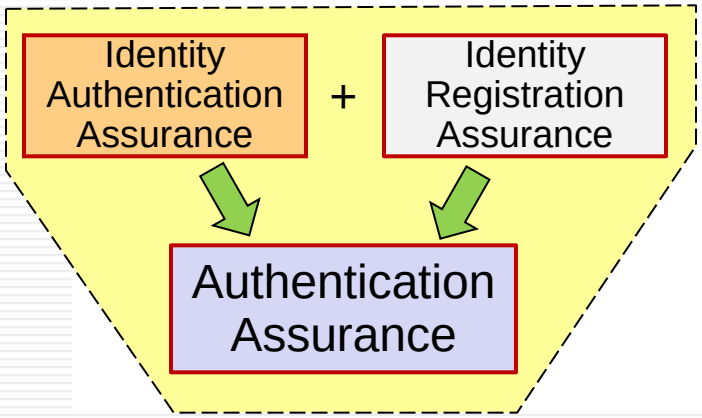
Example taken from Australian NeAF 2009

Identity Authentication Assurance Levels



Credential Management Assurance	Authentication Method Strength 1	2	3	4
4	Low (2)	Moderate (3)	High (4)	High (4)
3	Low (2)	Moderate (3)	Moderate (3)	High (4)
2	Low (2)	Low (2)	Moderate (3)	Moderate (3)
1	Minimal (1)	Low (2)	Low (2)	Low (2)

Authentication Assurance Levels



Identity Registration Assurance	0	1	2	3	4
4	None (0)	Pseudo-nymous Mininmal	Pseudo-nymous Low	Pseudo-nymous Moderate	Pseudo-nymous High
3		Minimal (1)	Low (2)	Moderate (3)	Moderate (3)
2		Minimal (1)	Low (2)	Low (2)	Low (2)
1		Minimal (1)	Minimal (1)	Minimal (1)	Minimal (1)
0		Minimal (1)	Low (2)	Moderate (3)	High (4)

Identity Authentication Assurance

Comparison of Assurance Levels

	Assurance Levels				
IDA (EU)	N/A	Minimal (1)	Low (2)	Substantial (3)	High (4)
NeAF (Au)	None (0)	Minimal (1)	Low (2)	Moderate (3)	High (4)
NIST (US) FADS (Norw.)	Little or None (1)		Some (2)	High (3)	Very High (4)
UKOnline	Minimal (0)	Minor (1)	Significant (2)	Substantial (3)	

- IDA: Interchange of Data between Administrations
- NeAF: National e-Authentication framework
- NIST: National Institute of Standards and Technology
- FADS: Framework for Authentication and Digital Signatures

Authentication assurance options Level 1 (FADS Norway)

- Online self-registration and self-chosen password
- Pre-authentication by providing person number

Provides little or no authentication assurance

Authentication assurance options Level 2 (FADS Norway)

- Fixed password provisioned in person or by mail to user's address in national person register
- OPT calculator without PIN, provisioned in person or by mail to address in national person reg.
- List of OTP (one-time passwords) provisioned in person or by mail to address in national pers. reg.

Provides some authentication assurance

Authentication assurance options Level 3 (FADS Norway)

- OTP calculator with PIN provisioned separately in person or by mail to address in national pers. reg.
- SMS-based authentication, where enrolment of mobile phone is based on code provisioned in person or by mail to address in national pers. reg.
- Personal public-key certificate with gov. PKI
- List of OTP (one-time passwords) combined with static password and username provisioned in person or by mail to address in national pers. reg.

Provides high authentication assurance

Authentication assurance options Level 4 (FADS Norway)

- Two-factor, where at least one must be dynamic, and at least one is provisioned in person (the other by mail to address in national pers. reg. Also requires logging and auditing by third party.
- Same as above, but uses trusted system instead of third party logging.

No adequate technology/standardisation currently exists for implementing Level 4 assurance.

Provides very high authentication assurance.

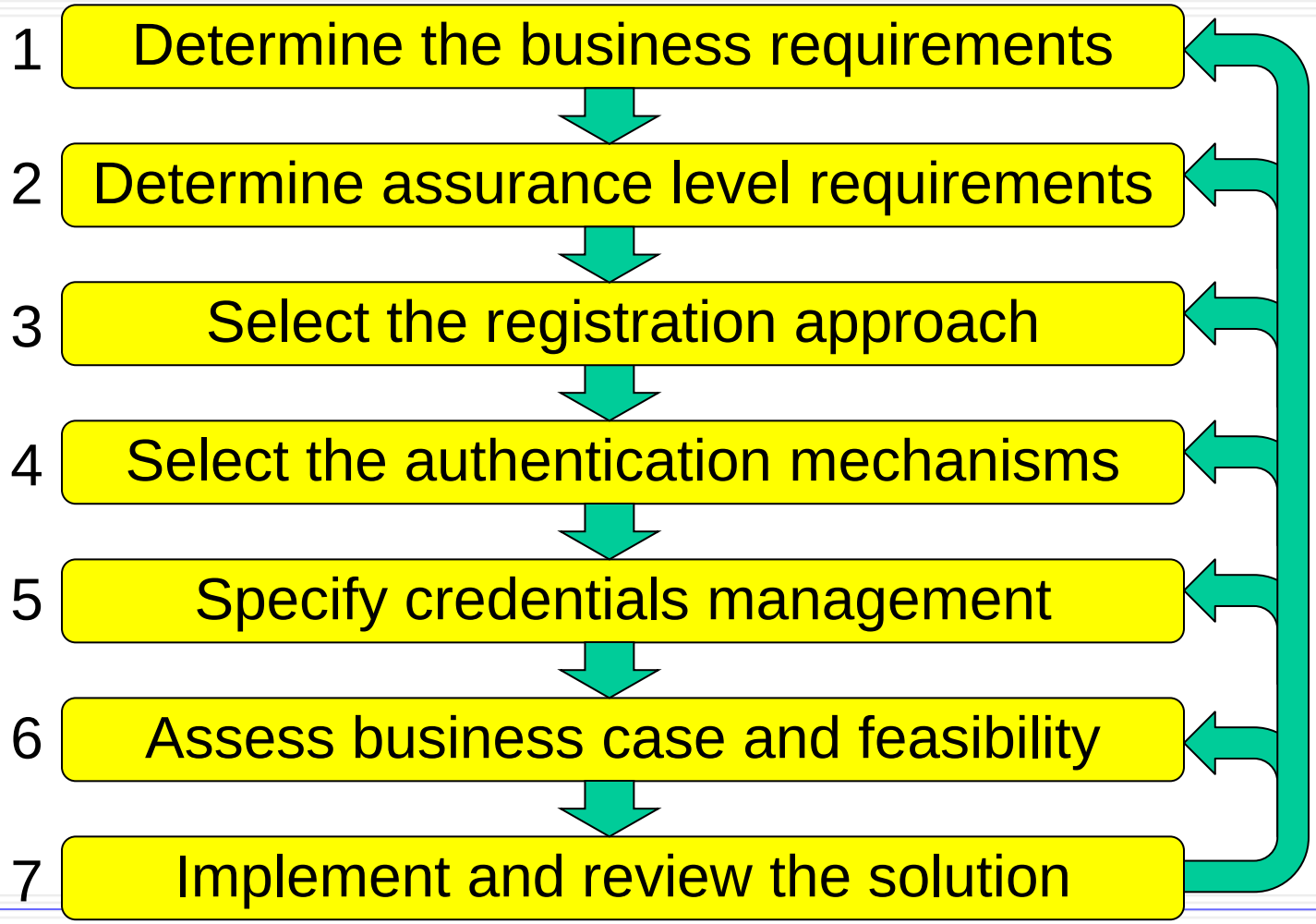
Risk Analysis for Authentication

Determines required Authentication Assurance Level

		Impact of e-Authentication failure				
		Insignificant	**Minor**	**Moderate**	**Major**	**Severe**
Likelihood	**Almost Certain**	None (0)	Low (2)	Moderate (3)	High (4)	High (4)
	Likely	None (0)	Low (2)	Moderate (3)	High (4)	High (4)
	Possible	None (0)	Minimal (1)	Low (2)	Moderate (3)	High (4)
	Unlikely	None (0)	Minimal (1)	Low (2)	Moderate (3)	Moderate (3)
	Rare	None (0)	Minimal (1)	Low (2)	Moderate (3)	Moderate (3)

Example: NeAF Australia

Steps of an Authentication Framework

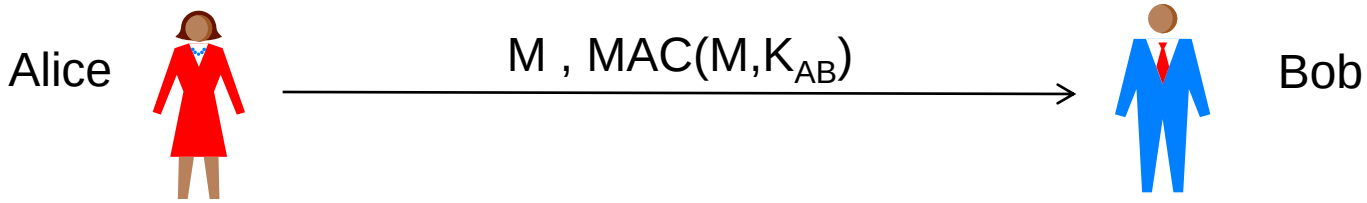


Message Authentication

Verifying the origin of data

Authentication and Non-Repudiation

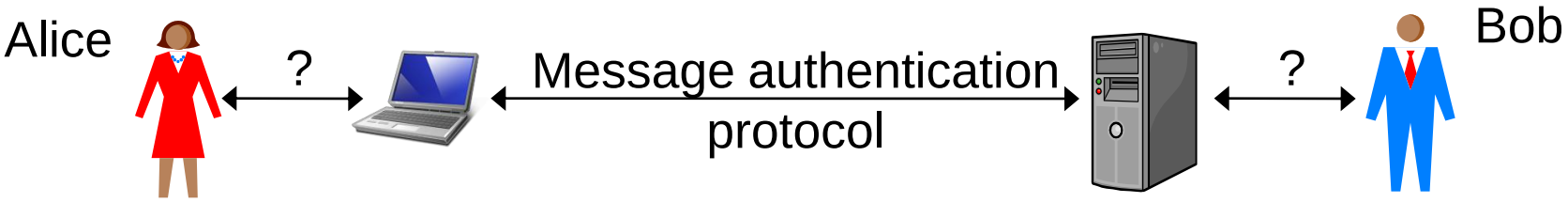
- Message authentication between two parties can rely on a shared secret using encryption or MAC



  - Bob is convinced that the message came from Alice
  - However, Bob can not convince any third party that the message came from Alice
- To convince a third party (e.g. a court) about message origin, non-repudiation is required
  - Requires e.g. a digital signature

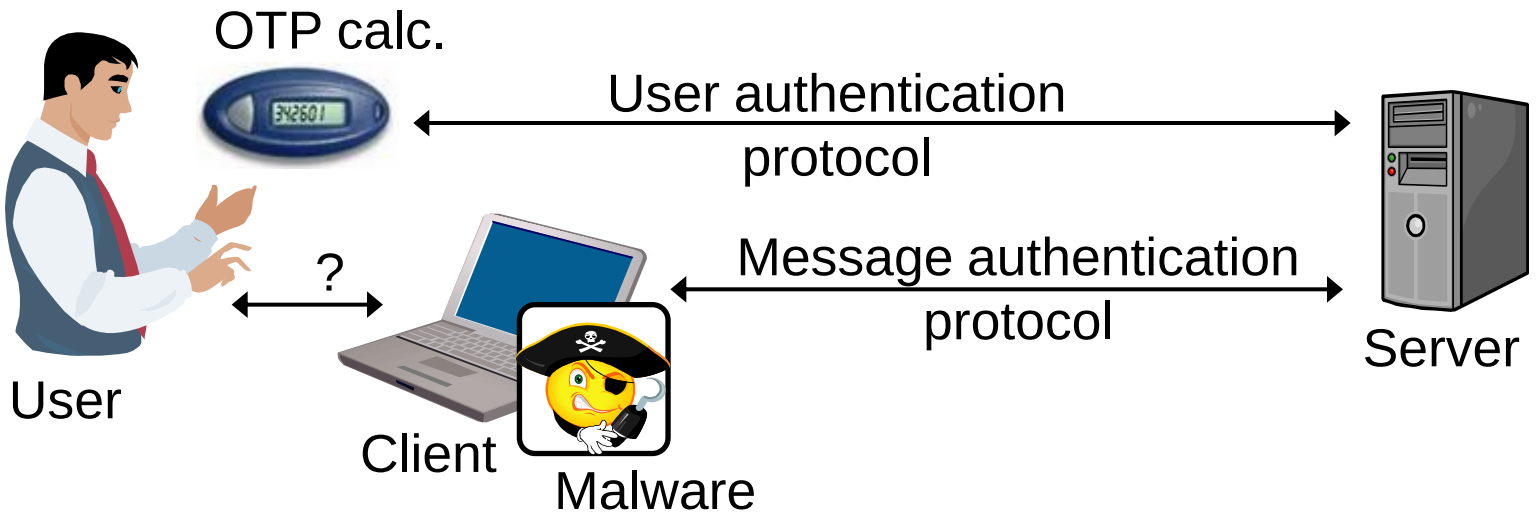
The Alice-&-Bob Fallacy

- Message authentication theory assumes that Alice and Bob perform cryptographic operations
- In reality, client and server computers do that.



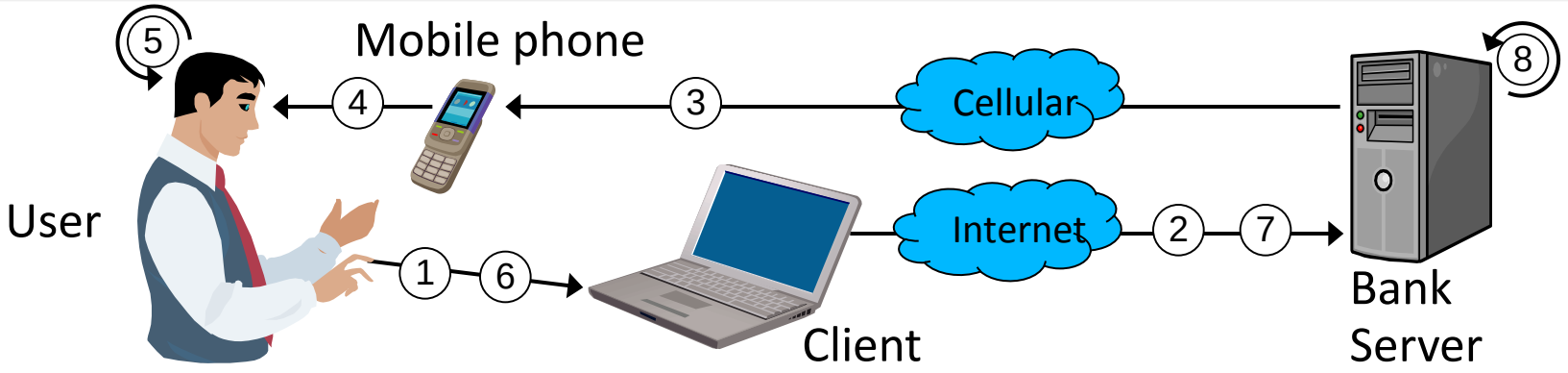
- Difficulty of verifying cryptographic operations inside computers makes it difficult to achieve meaningful message authentication

Failure of user authentication to prevent attack on message authentication



- In case of malware attack, the server “authenticates” messages from malware/attacker, not from user.
- Semantically, this is **not** message authentication
- User authentication does not prevent this attack

Combined user and message authentication through integrated dual-channel protocol



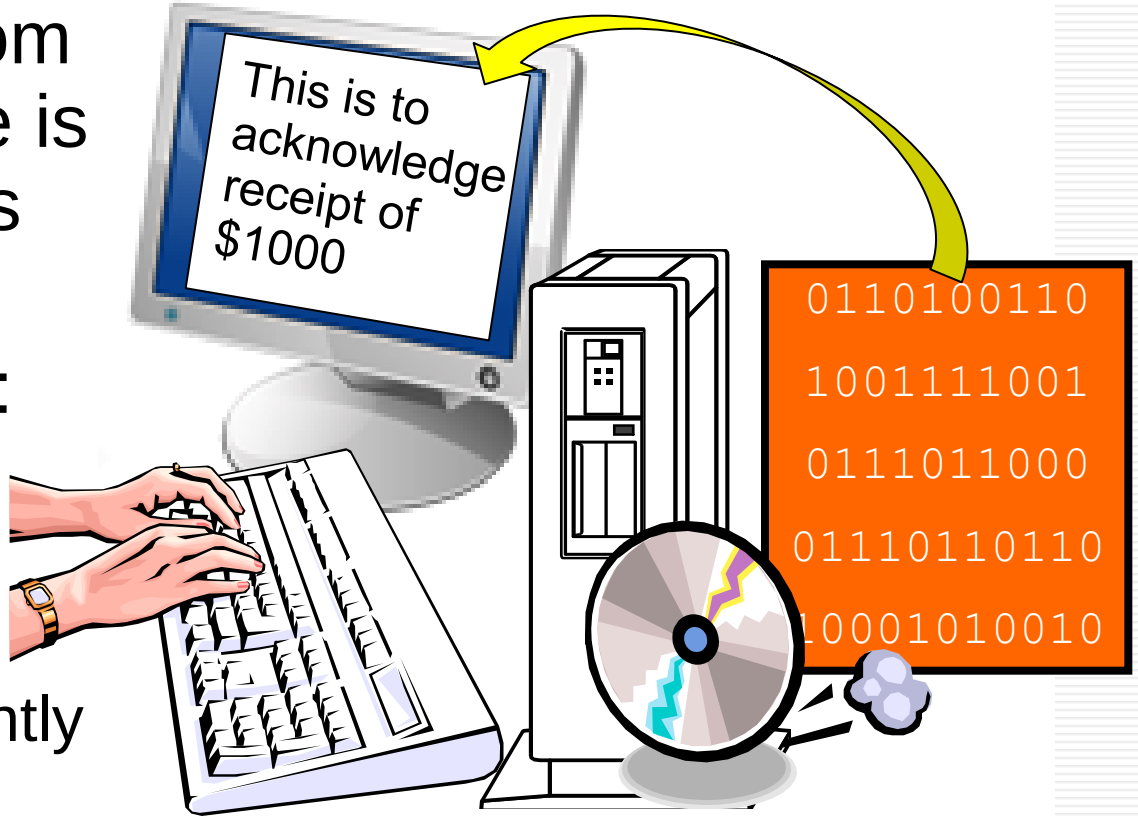
1. Specify destination account and amount
2. Transaction data transmission
3. SMS with authentication code, destination account and amount
4. View SMS
5. Verify transaction data in SMS
6. If transaction is correct, copy authentication code to browser
7. Transmit authentication code
8. Verify authentication code. If OK, execute transaction.

WYSIWYS for digital signatures (What You See Is What You Sign)

- WYSIWYS means that the semantic interpretation of a signed message, such as analogue display, cannot be changed. In particular this also means that a message cannot contain hidden info that the signer is unaware of, and that can be revealed after the signature has been applied.
- WYSIWYS is a desirable property of digital signatures that is extremely difficult to guarantee because of the increasing complexity of modern computer systems.

Binary-analogue semantic distance

- Transformation from binary to analogue is a complex process
- No guarantee for equivalent display:
  - Replaced fonts
  - Malware infection
  - XML and HTML interpreted differently
- No guarantee for WYSIWYS



Acceptance of Digital Signatures

- Requires that a digital signature can be linked to a person with high certainty. Technically, this leads to requirements how:
  - cryptographic keys are generated
  - private keys are protected
  - digital signatures are generated and linked to the semantics of the information to be signed
  - public keys are linked to persons and attributes through third party certificates
  - authorized time stamps are used
  - publication an revocation of certificates is done
  - binary documents are transformed and interpreted

Digital signature evolution

- Early optimism in 1990s that digital signatures would replace hand-written signatures
- Political ambition for legal recognition
- Problems with PKI and with the integrity platforms have demonstrated that digital signatures have serious vulnerabilities
- Digital signature does not represent a practical widely and legally accepted method for non-repudiation

Legal Aspects

- Initiatives to get recognition of digital signatures in the legal system
- Legal issues seem even harder to solve than any technical problem
- Affects cultural habits and values grown over centuries
- Plethora of different legal systems in the world
- Digital signature legislation on the way in many countries (e.g. Germany, Canada, Australia, Singapore, Italy, Austria, several US states, EU)
- BUT digital signatures must work globally

EESSI Charter

- EESSI: European Electronic Signature Standardisation Initiative
- Electronic Signature Directive is providing a common EU framework for electronic signatures
- Industry, with the assistance of European Standards Bodies, to provide an agreed framework for an open, market-oriented implementation of the Directive
- EESSI has had limited progress

Electronic Signatures

- Not the same as digital signature
- Electronic signature can be:
  - Name written in email message
  - Log of an electronic transaction
  - Sender phone number of SMS message
- Represents evidence of computer actions
- Strength of evidence depends on integrity and forensic chain of custody

Review

- The meaning of authentication and identity
- Difference between user authentication and message authentication
- User authentication methods
- Message authentication
- Digital signature strength and recognition