INF3510 Information Security
University of Oslo
Spring 2010

Lecture 4

Authentication

Audun Jøsang

Outline

- Concepts related to authentication
- User Authentication
  - Knowledge-Based Authentication
    - Passwords
  - ID-Based Authentication
    - Biometrics
  - Object-Based Authentication
    - Tokens
- Message Authentication
  - Electronic and Digital Signatures
  - Standardisation 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:

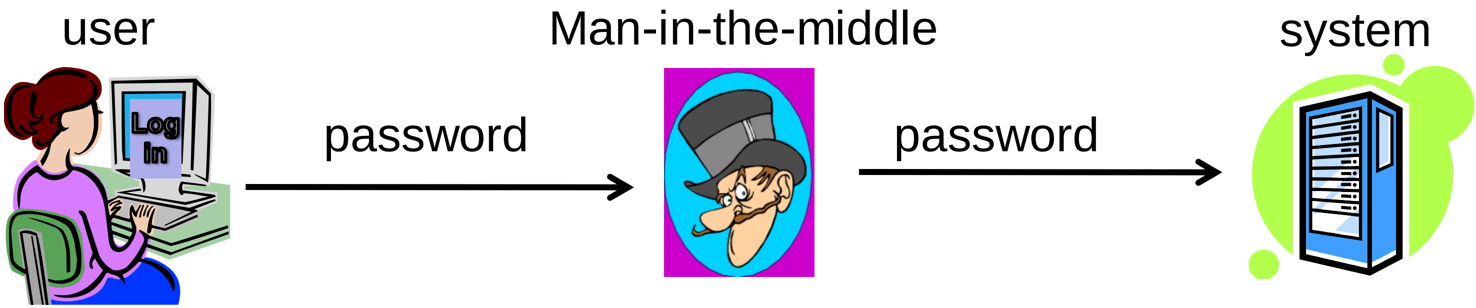
Message Authentication

User or 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. a digital certificate)

User or 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 every received message originates from the user/entity or terminal.
  - Somebody else can take over the terminal or session
  - There can be a man-in-the-middle attack



user

password

Man-in-the-middle

password

system

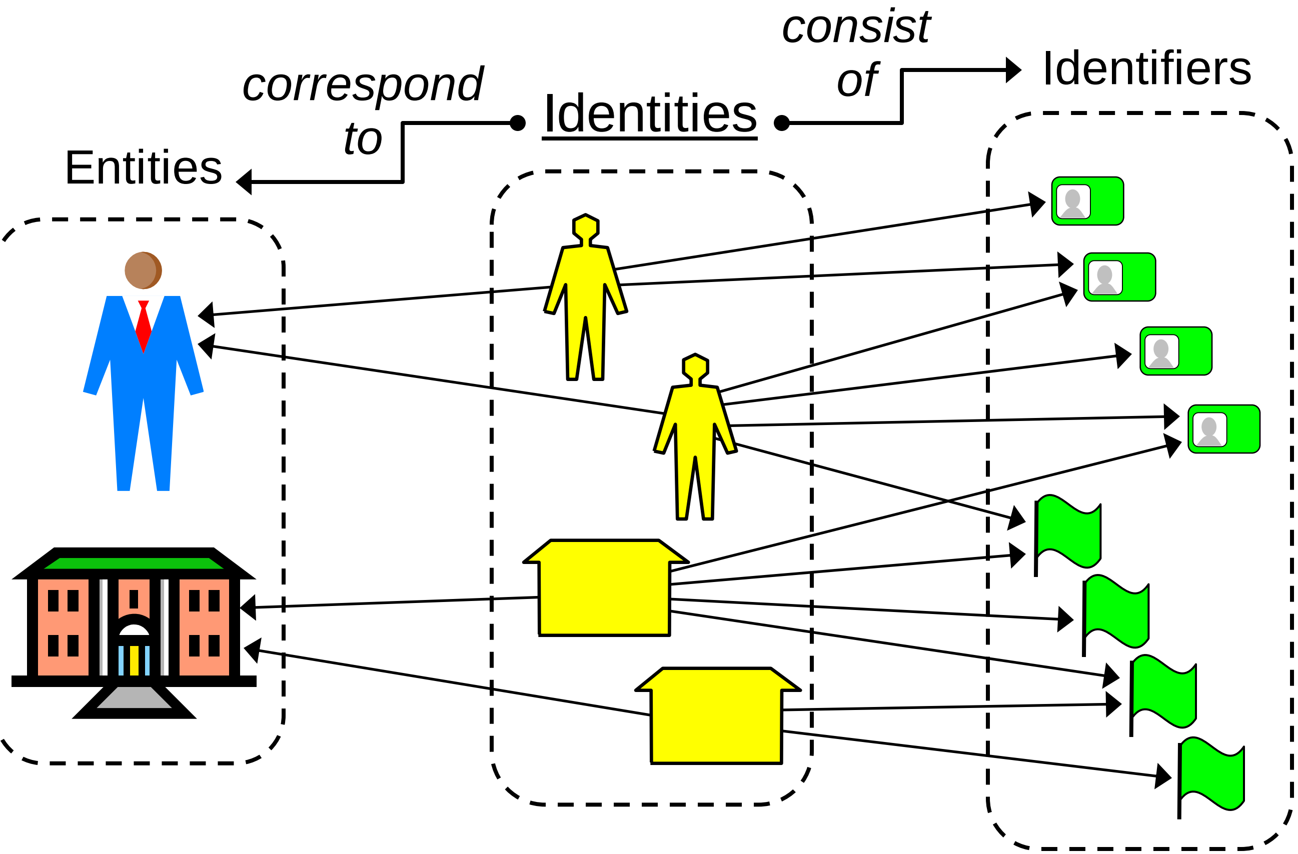
Data Origin or Message Authentication

- 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

- Authentication requires identity
  - "*peer entity*" (user identity)
  - "*source of data*" (sender identity)
- What is the identity of a user? or a sender?
  - What about: "Mr. Apple", "apple123@hotmail.com", "www.apple.com", www.applecorp.com, "193.156.98.149", "apple computers", "apple records" ?
- It is essential to know the meaning of identity to properly understand the meaning and significance of authentication.

The Concept of Identity



Concepts related to identity

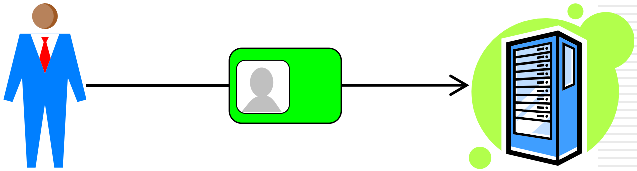
- Entity
  - A person, organisation, agent, system, etc.
- Identity
  - A set of characteristics of an entity in a specific domain
  - An entity may have multiple identities in one domain
- Digital identity
  - Identity resulting from digital codification of identifiers in a way that is suitable for processing by computers
- Identifier
  - A characteristic or attribute
    - Can be unique or ambiguous (non-unique) within a domain
    - Transient or permanent, self defined or by authority, suitable for interpretation by humans and/or computers, etc

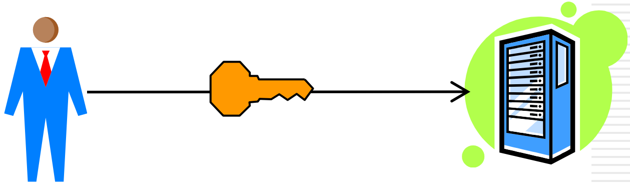
User/Entity Authentication

Stages of User Authentication

1. Identification
   - Present a unique identifier to select identity
2. Verification of identity
   - Produce an authenticator as proof of identity

- An alternative model can be that the authenticator also is the identifier
  - Requires that the authenticator is unique.





Authentication: Types of entities

- Human authentication:
  - Performed to verify that the claimed identity of a person is the true identity
  - What is identity?
- Machine
- Document
- Origin
- Roles authenticated include:
  - Client,
  - Server,
  - Mutual

Authenticators: Overview

- The ‘thing’ used to perform authentication is called an authenticator.
  - Reusable passwords, Biometrics, Smart cards, 1-time tokens are all authenticators.
  - May also be referred to as a token or credential.
- 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

Authenticators : Categories

- Knowledge-Based (Something you know):
  - Characterized by secrecy or obscurity.
  - This type includes a memorized password.
  - Also includes “Mother’s maiden name” and your dog’s name.
  - Could be a secret key.
  - Can be shared.
  - Difficult to know if compromised.

Authenticators : Categories

- Object-Based (Something you have):
  - Characterized by physical possession of a token.
  - For example a house key.
  - Difficult to share (effort required to make a copy).
  - If lost, the finder can make use of the token.
  - If lost, the owner sees evidence of the loss.

Authenticators : Categories

- ID-Based (Something you are):
  - Characterized by uniqueness to one person.
  - Examples include:
    - photo-id
    - biometrics such as a fingerprint, eye scan, voiceprint, signature, gait
  - Security is based on the difficulty of copying or forging the ID.
  - If a biometric is compromised or a document is lost, they are not as easily replaced as passwords or tokens.

Authenticators : Categories

- Location-based (Somewhere you are)
  - Characterized by location (space and time?)
  - It might involve location and tracking technologies such as the triangulation of cell-phone signals or the use of global positioning systems (GPS).
  - Machine IP address is a crude location attribute as is DNS name
  - Time as an authenticator
  - Privacy issues

Authentication: Multi-factor

- Multi-factor authentication aims to combine two or more authentication techniques in order to form a stronger and more reliable level of authentication.
- 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: ATM PIN and card

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.

Authentication: Password selection strategies

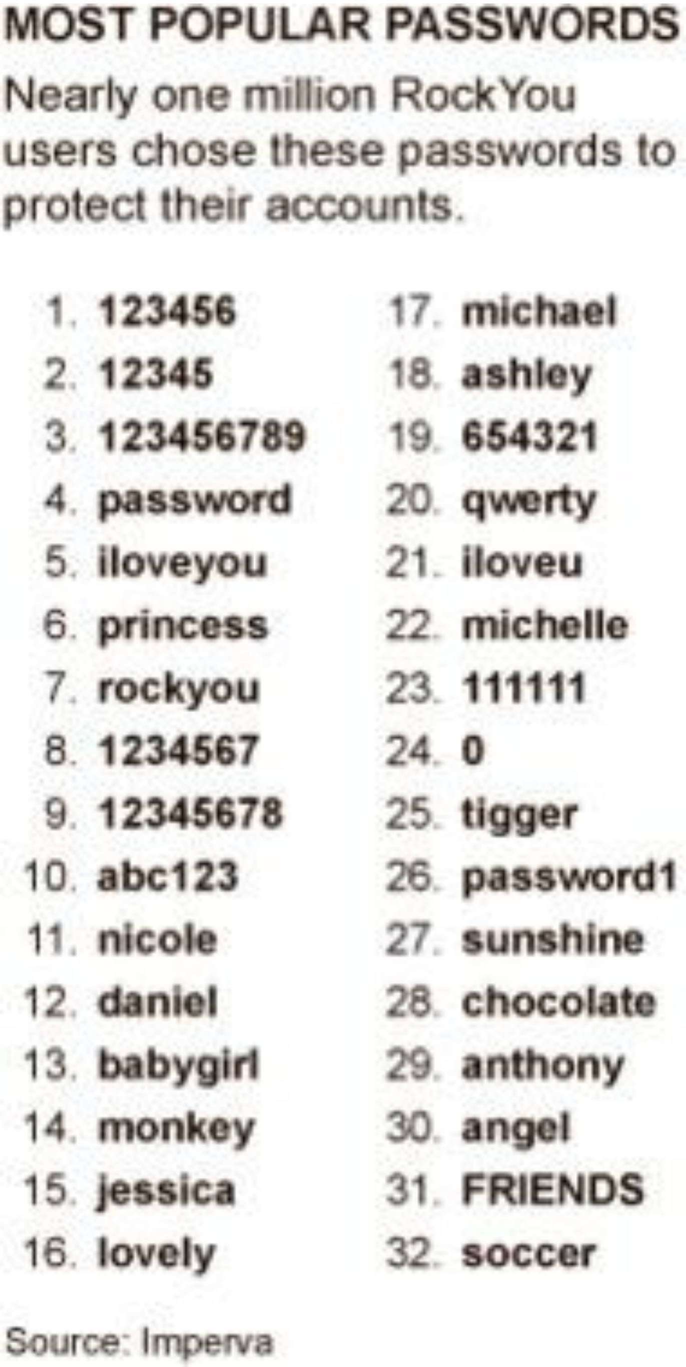
- User education
- Computer-generated passwords
- Reactive password checking
- Proactive password checking

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

- If the ‘clear’ password is captured during transmission, an attacker may reuse the password and masquerade as the client.
- An attacker masquerading as the server can get the password from the user
  - E.g. phishing attack.
- Solutions to these problems include:
  - Password encryption
  - One-time passwords
  - Challenge-response protocols
  - Server authentication

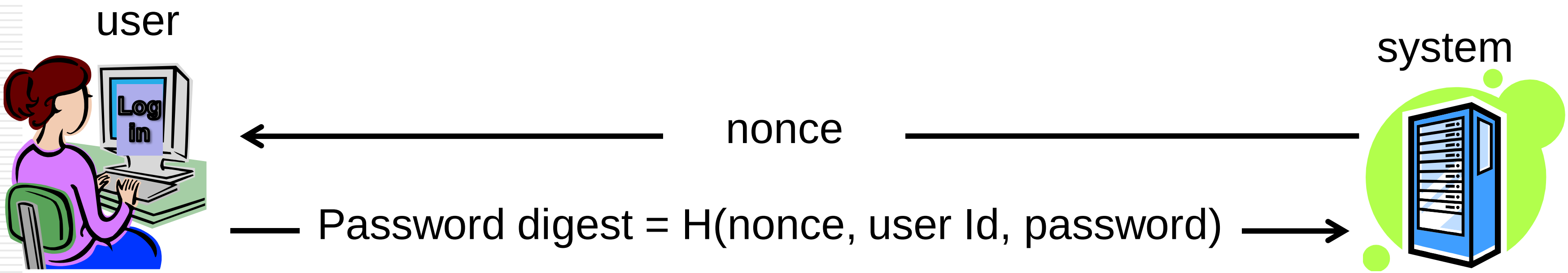
Authentication: Challenge-Response Mechanisms

- A common mechanism used to avoid sending passwords in the clear is to use a Challenge-Response protocol.
- The entity to be authenticated must respond to a challenge by correctly performing a calculation based on knowledge of the password.
- Examples:
  - CHAP, MS-CHAP
  - HTTP Digest Authentication
  - CRAM
  - APOP

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



user

system

nonce

Password digest = H(nonce, user Id, password)

OTP: One-time passwords

- OTP described in RFC 2289 (1998)
  http://www.faqs.org/rfcs/rfc2289.html
  - Aims to be secure against passive attacks based on replaying captured reusable passwords.
  - The security of the OTP system is based on the non-invertibility of a secure cryptographic hash function.
  - Uses a hash chain
  - Often implemented as a ‘soft’ token

OTP: Operational Overview

- Uses a secret pass-phrase to generate a sequence of one-time (single use) passwords.
- The user's secret pass-phrase never needs to cross the network at any time such as during authentication or during pass-phrase changes.
  - Thus, it is not vulnerable to replay attacks.
- Added security is provided by the property that no secret information need be stored on any system, including the server being protected.
  - Note: Hash values are encoded as pronounceable words

ID-Based Authentication

Something you are: Biometrics

Biometrics: Overview

- Why use it?
  - convenient as cannot 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

- Security Drivers
  - national border security,
  - preventing ID theft,
  - enterprise-wide network security infrastructures,
  - secure electronic banking,
  - investing and other financial transactions,
  - retail sales,
  - law enforcement, and
  - health and social services

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.

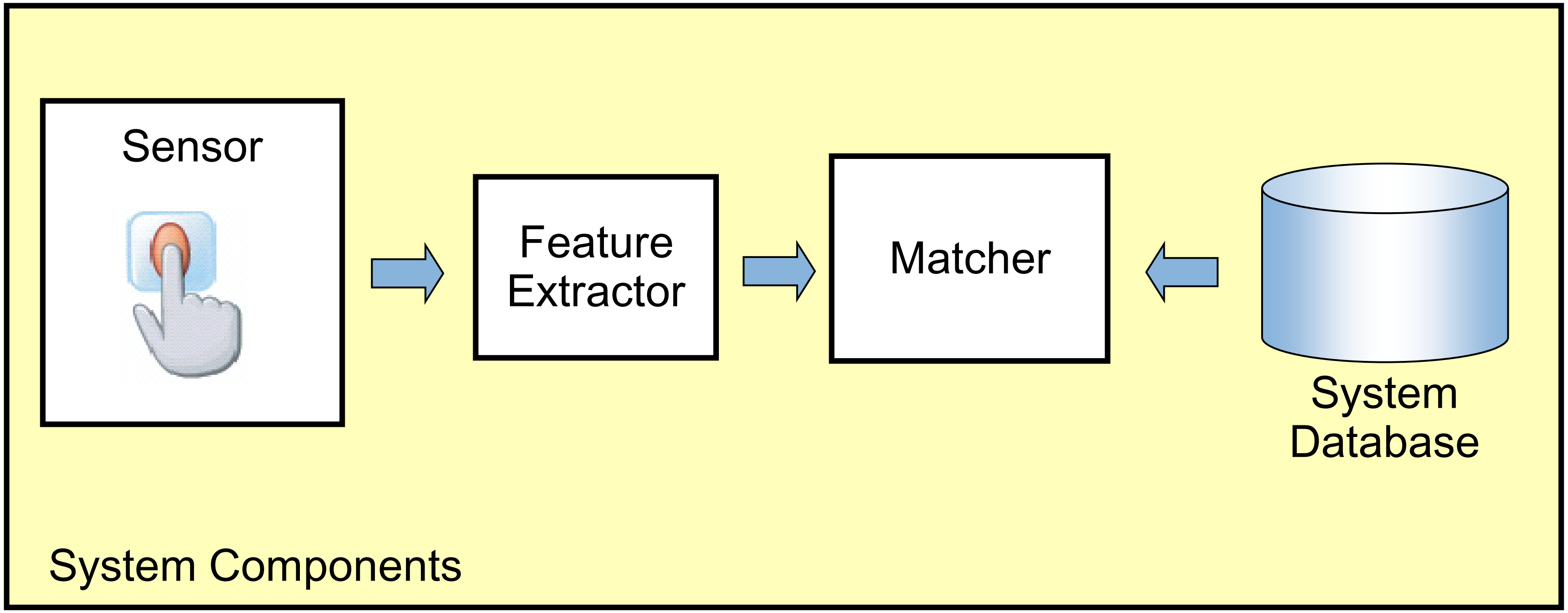
Biometrics: Practical considerations

- 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:
Uses

- Where could biometric-based authentication be used?
  - workstation, network, and domain access,
  - single sign-on,
  - application logon,
  - data protection,
  - remote access to resources,
  - transaction security and
  - Web security

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.

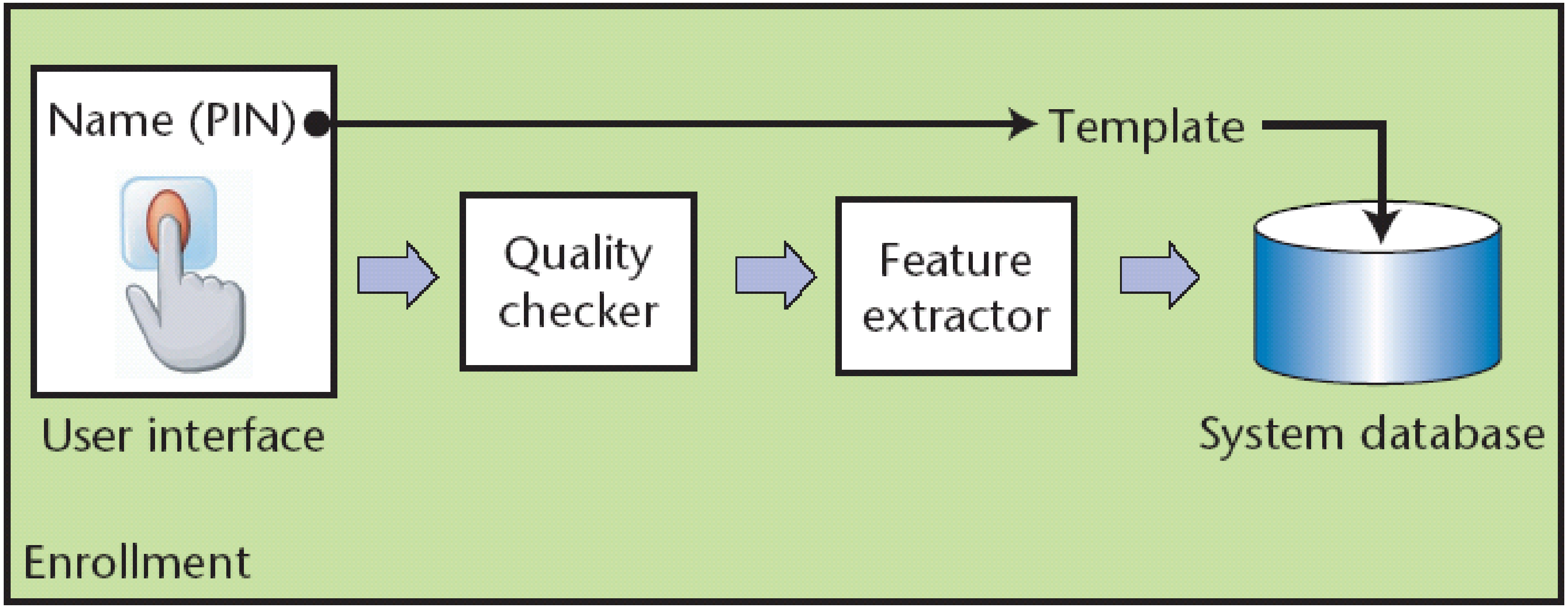
Biometrics: System components

- 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

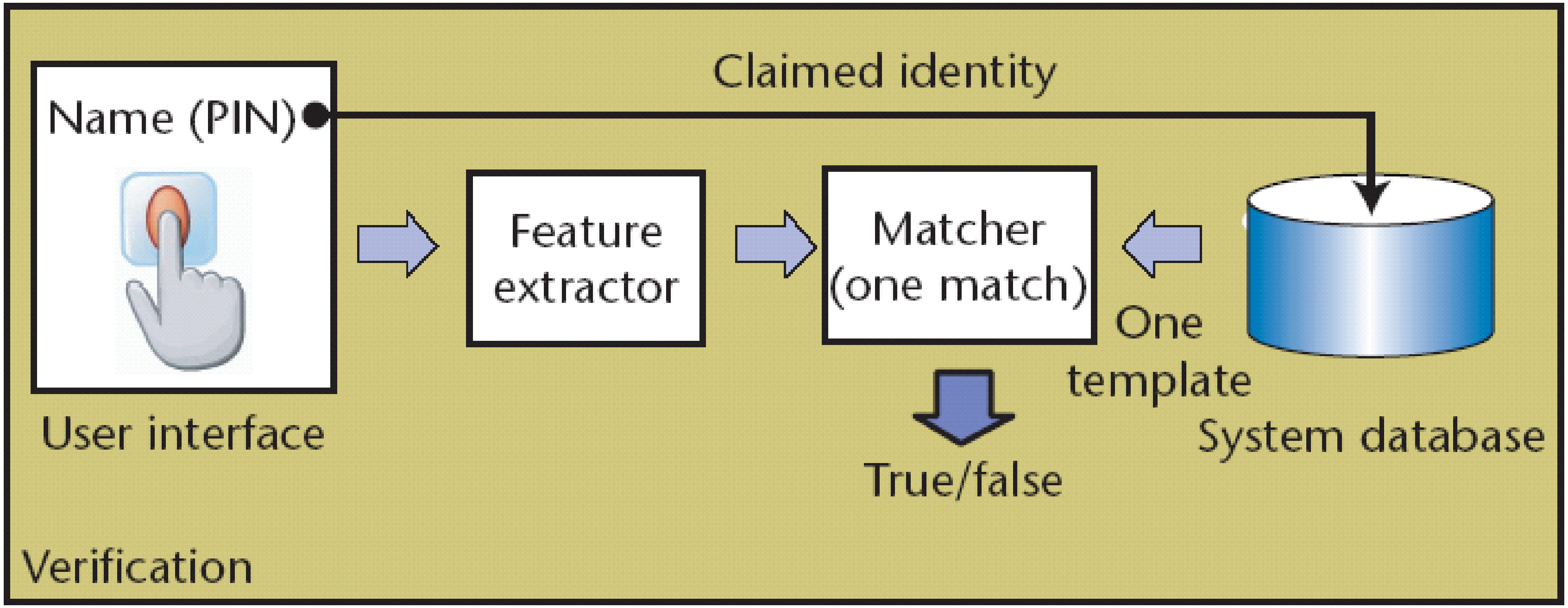
- Enrolment:
  - analog capture of the user’s biometric attribute.
  - processing of this captured data to develop a template of the user’s attribute which is stored for later use.
- Identification (1-to-many):
  - capture of a new biometric sample.
  - search the database of stored templates for a match 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



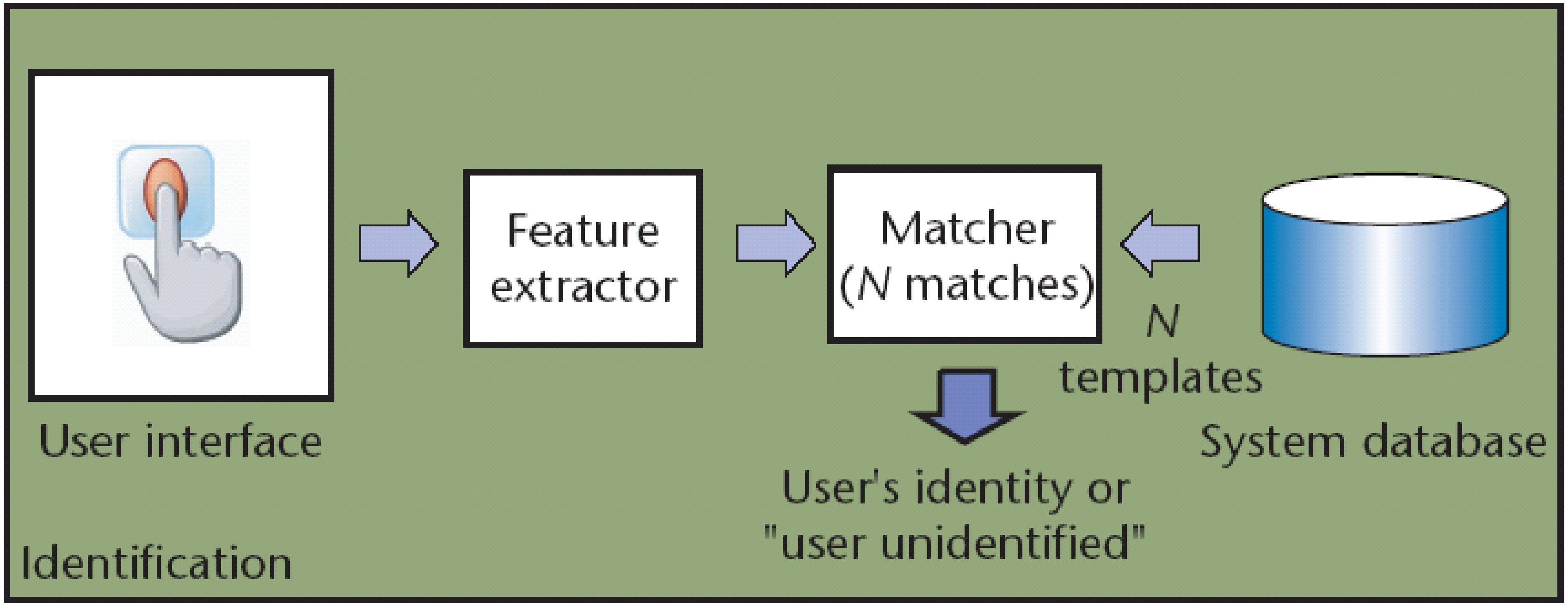
Source: Biometric Recognition: Security and Privacy Concerns

Biometrics: Verification



Source: Biometric Recognition: Security and Privacy Concerns

Biometrics: Identification



Source: Biometric Recognition: Security and Privacy Concerns

Biometrics Types: Classification

- Stable:
  - Relatively constant in time except for minor perturbations due to noise (and excluding drastic obfuscation by accident or plastic surgery).
  - What if someone can forge a stable biometric?
  - Examples: Fingerprints, Facial recognition, Eye retina/iris scanning
- Alterable:
  - Comprised of two components, the underlying stable biometric and some variable.
  - For example, saying or writing a given word
  - What if someone can forge an alterable biometric?
  - Examples: Voice

Biometrics Types: Fingerprints

- Stable biometric. Non-intrusive?
- Based on the fact that the patterns of friction ridges and valleys on an individual's fingertips are unique.
- Pre-dates computers in law enforcement.
- Fingerprint recognition devices for desktop and laptop access are now widely available
- Early methods were optical - a camera-like device collects a high-resolution image of a fing

Biometrics Types: Weaknesses of fingerprints

- A clear repeatable image of the fingerprint pattern is required.
- In the real world this is not a trivial task.
  - harsh chemicals and physical wear may damage the patterns on the surface of our fingers.
  - reader may become worn and dirty and hence unreliable.
  - finger must be live.
  - acceptance (germ transmission issues)

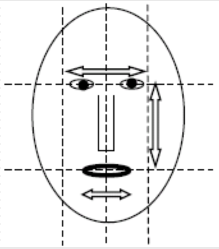
Biometrics Safety

- 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

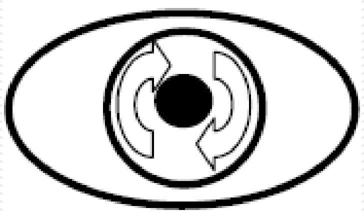
(NST picture by Mohd Said Samad)

Biometrics Types: Facial recognition



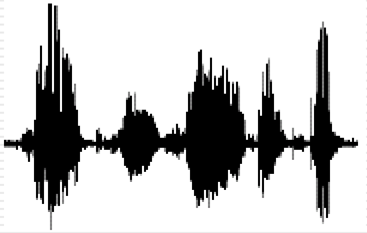
- Non-intrusive stable biometric method
- Most common biometric characteristic used by humans to make a personal recognition.
- The applications of facial recognition range from a static, controlled “mug-shot” verification to a dynamic, uncontrolled face identification in a cluttered background (e.g., airport).
- Usually based on either
  - the location and shape of facial attributes, or
  - the overall (global) analysis of the face image as a weighted combination of a number of canonical faces.

Biometrics Types: Iris scanning



- Stable biometric. Intrusive?
- Each iris is distinctive and, like fingerprints, even the irises of identical twins are different.
- It is extremely difficult to surgically tamper with the texture of the iris.
- Newer systems have become more user-friendly and cost-effective.
- Trial being deployed at various UK airports as part of UK eBorders program.

Biometrics Types: Voice



- Non-intrusive alterable biometric that combines physiological and behavioural characteristics
  - physiological characteristics of human speech (determined by vocal tracts, mouth, etc) are fixed.
  - The behavioural part changes over time due to age, illness, emotional state, etc
- Text-dependent and text-independent voice recognition systems:
  - Text-dependent: based on the utterance of a fixed text
  - Text-independent: recognizes the speaker independent of the words spoken.

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

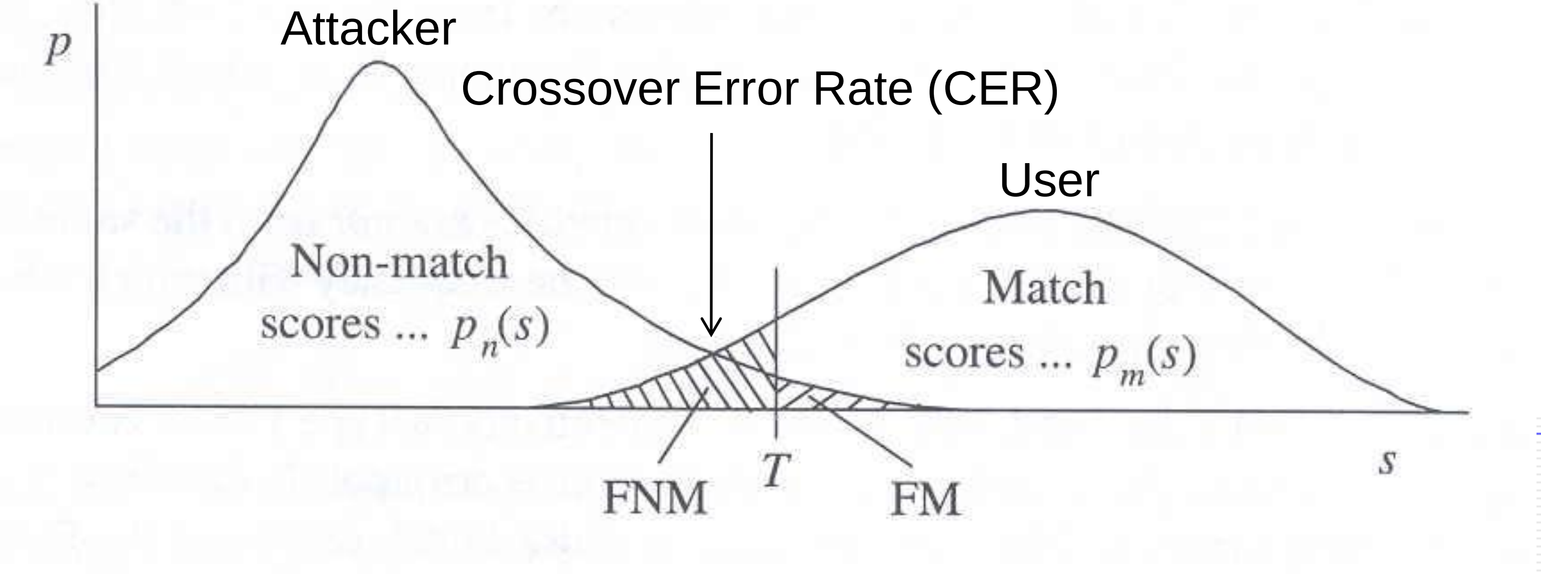
- Features captured during recognition are compared against the stored template
- The higher the score, the more certain is the system that the two biometric measurements come from the same person.
- The system decision is tuned by threshold t:
  - pairs of biometric samples generating scores higher 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

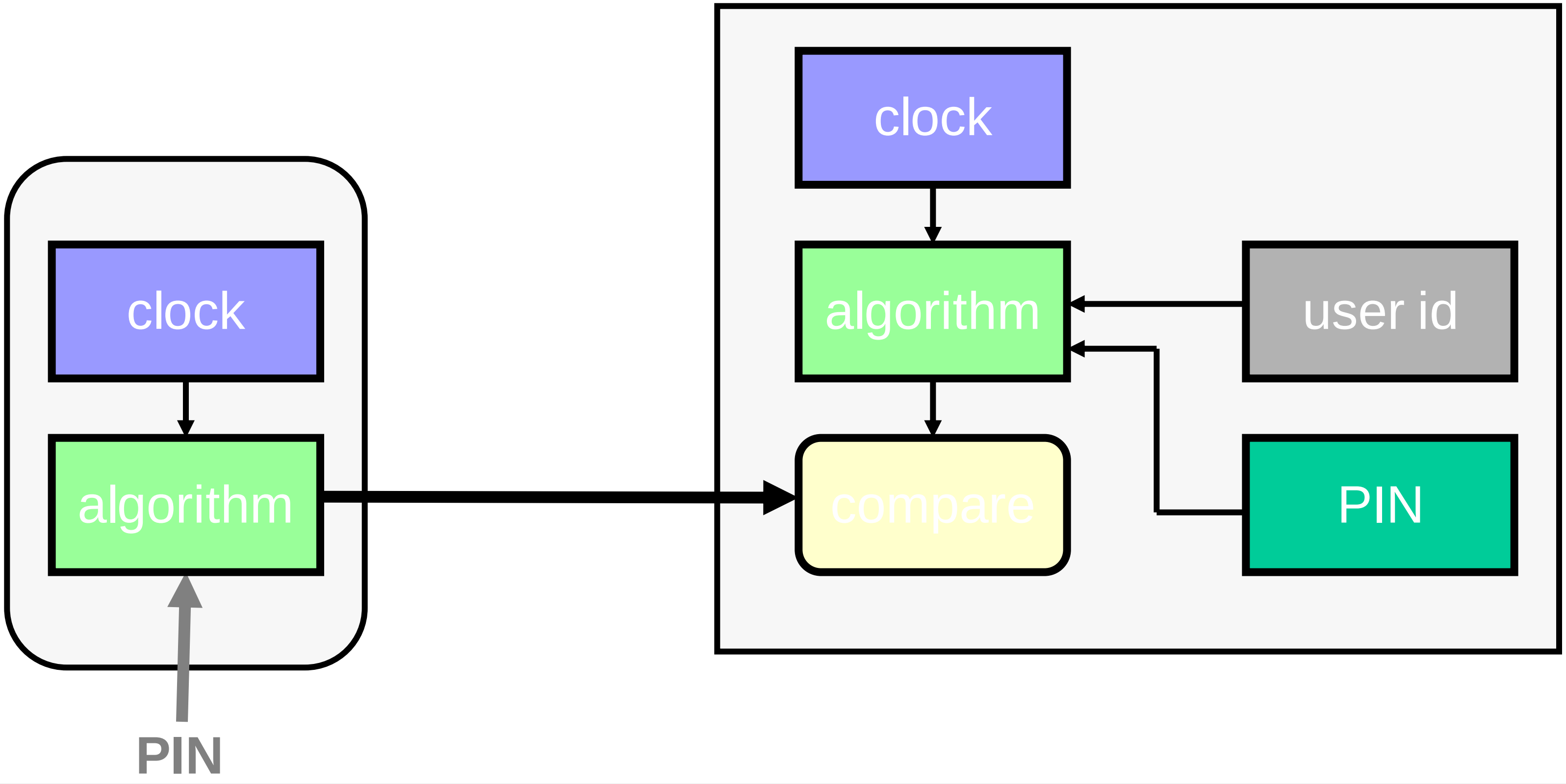
Synchronised Password Generator: Introduction

- 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 Tokens: Operation

- Token displays constantly changing value on display
  - User types in current value to log in
- Possession of the token is necessary to know the correct value for the current time
- Clocks must be synchronised
- Example: SecurID

Clock-based Tokens: Operation



Clock-based Tokens: RSA SecurID Operation

- Each RSA SecurID authenticator has a unique symmetric key
- The key is used with a proprietary algorithm (SecurID Hash) to generate a new code every 30/60 seconds.
- The code is unpredictable and dynamic.
- Difficult for a hacker to guess the correct code at any given time.

Clock-based Tokens: RSA SecurID token models

RSA SecurID SD600

RSA SecurID SID700

RSA SecurID SD200

BlackBerry with
RSA SecurID software token

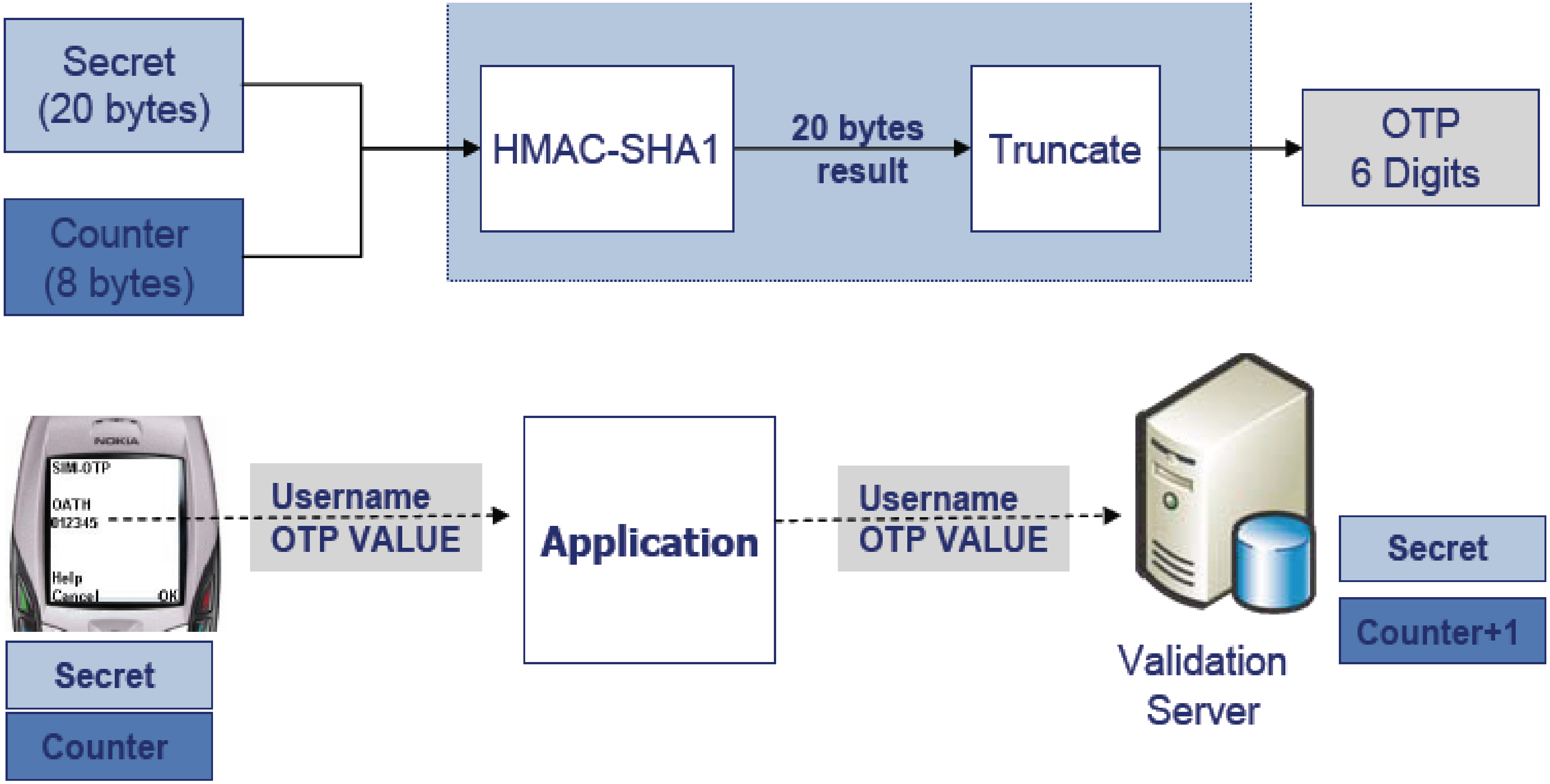
Clock-based Tokens: Issues

- The system fails if there is a loss of synchronisation between clocks.
- For network usage, there must be an acceptable window to allow for network delays
  - This opens up the possibility of an intermediate node capturing a password and logging in.

Counter-based 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

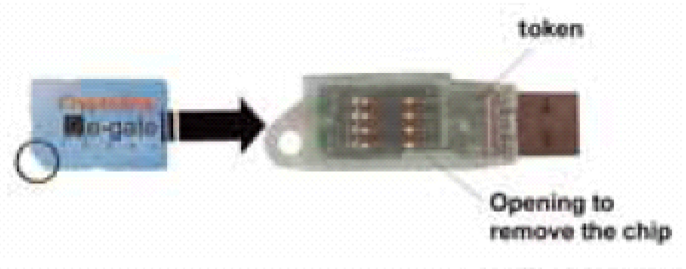
Counter-based Tokens: HOTP



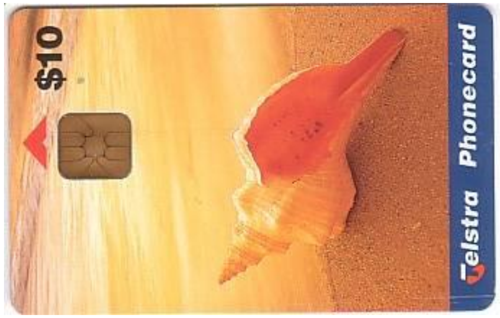
Smartcard Tokens: Overview

- Smart-card technology:
  Industry standard defined by the Joint Technical Committee 1 (JTC1) of the International Standards Organization (ISO) and the International Electronic Committee (IEC).
- Smartcards may
  - have contacts (ISO7816) or
  - be contactless (ISO 14443 and ISO 15693).

ICC with Contacts: Types



USB token

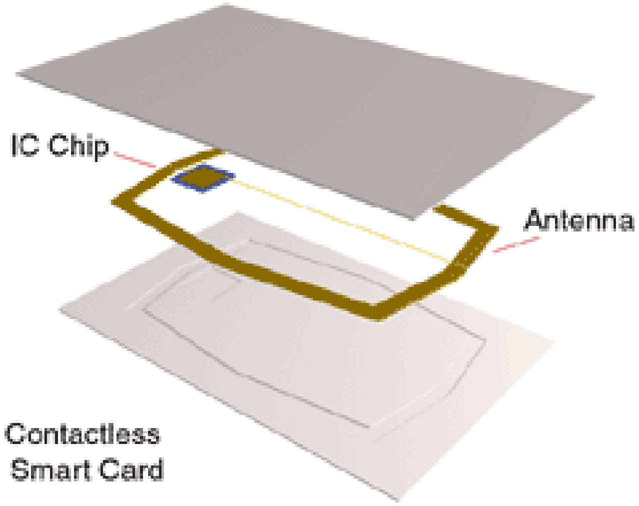


Java card

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



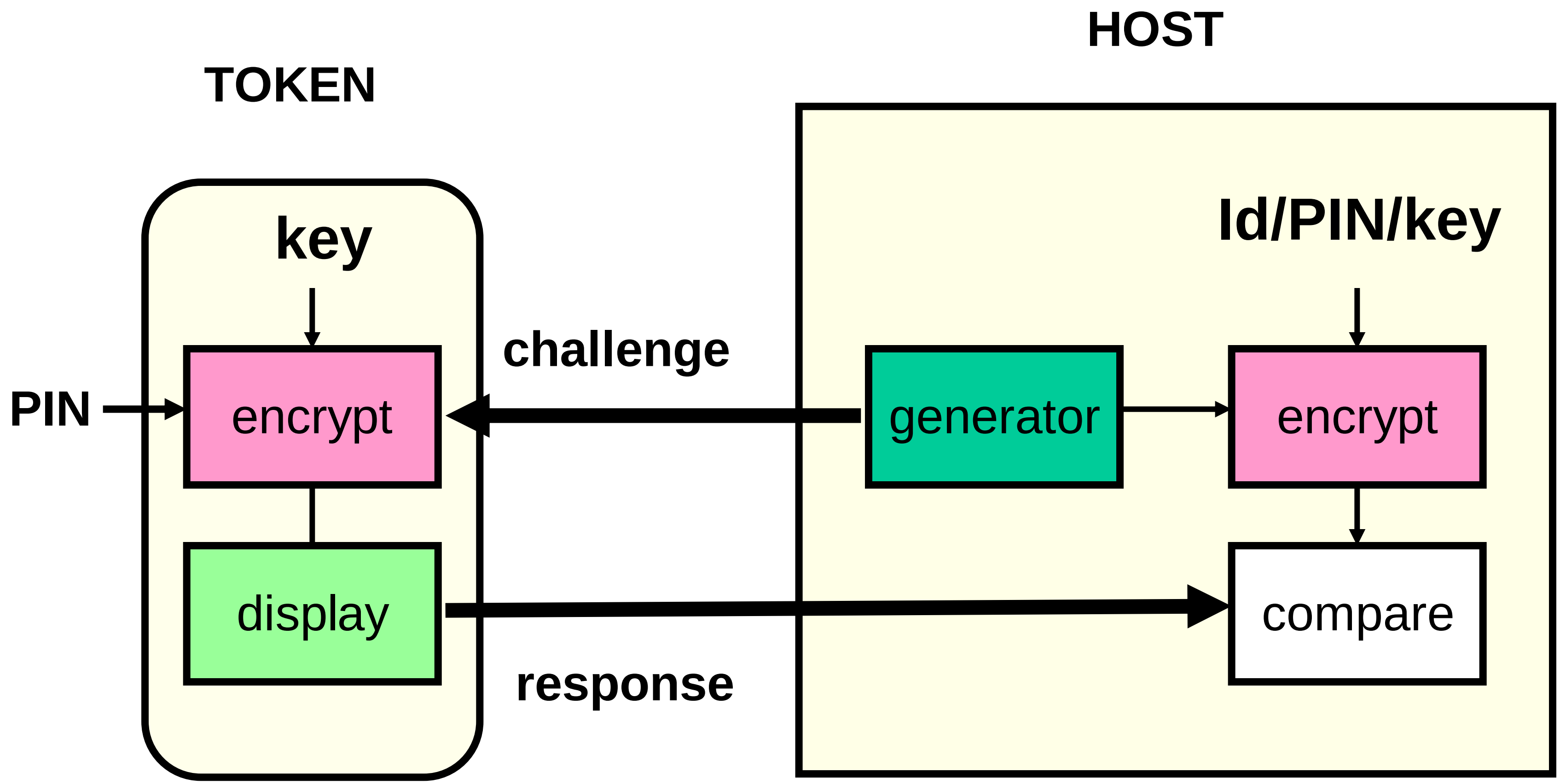
Token-based User Authentication: Challenge Response Systems

- A challenge is sent in response to an 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
  - If response is as expected by host, then access is granted
- 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

Token-based User Authentication: Challenge Response Systems

- Challenge is generally a number
- Response is computed as a cryptographic one-way function of challenge and other info such as key and PIN
- usually requires some computing device:
  - user types challenge into device
  - reads response off the device display,
  - and keys this response into the terminal
- Could use symmetric or asymmetric crypto

Token-based User authentication Challenge Response Systems



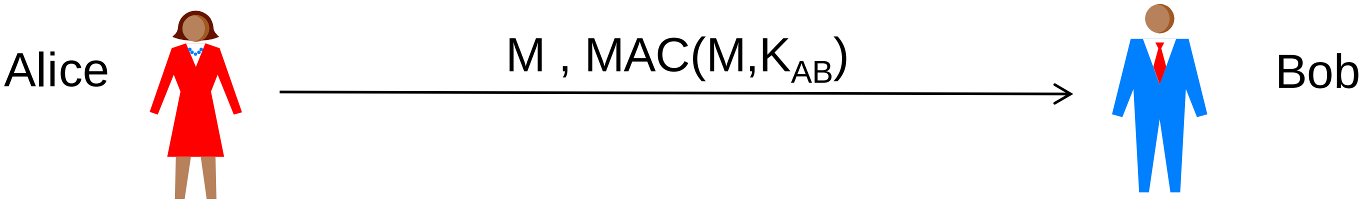
Symmetric Case

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

Legal Aspects

- Need to be able to use digital signatures in the legal system
- Problem much harder 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

Usability 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

European Electronic Signature Directive

- Legal recognition of electronic signatures (includes electronic and digital signatures)
- Technology neutral
- Free flow of Products and Services
- Forbids prior authorisation or licensing scheme for Certification Service Providers
- Mandates supervision scheme for CSPs (Certification Service Provider)

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 put in place to execute this task (ICT-SB Dec.98)

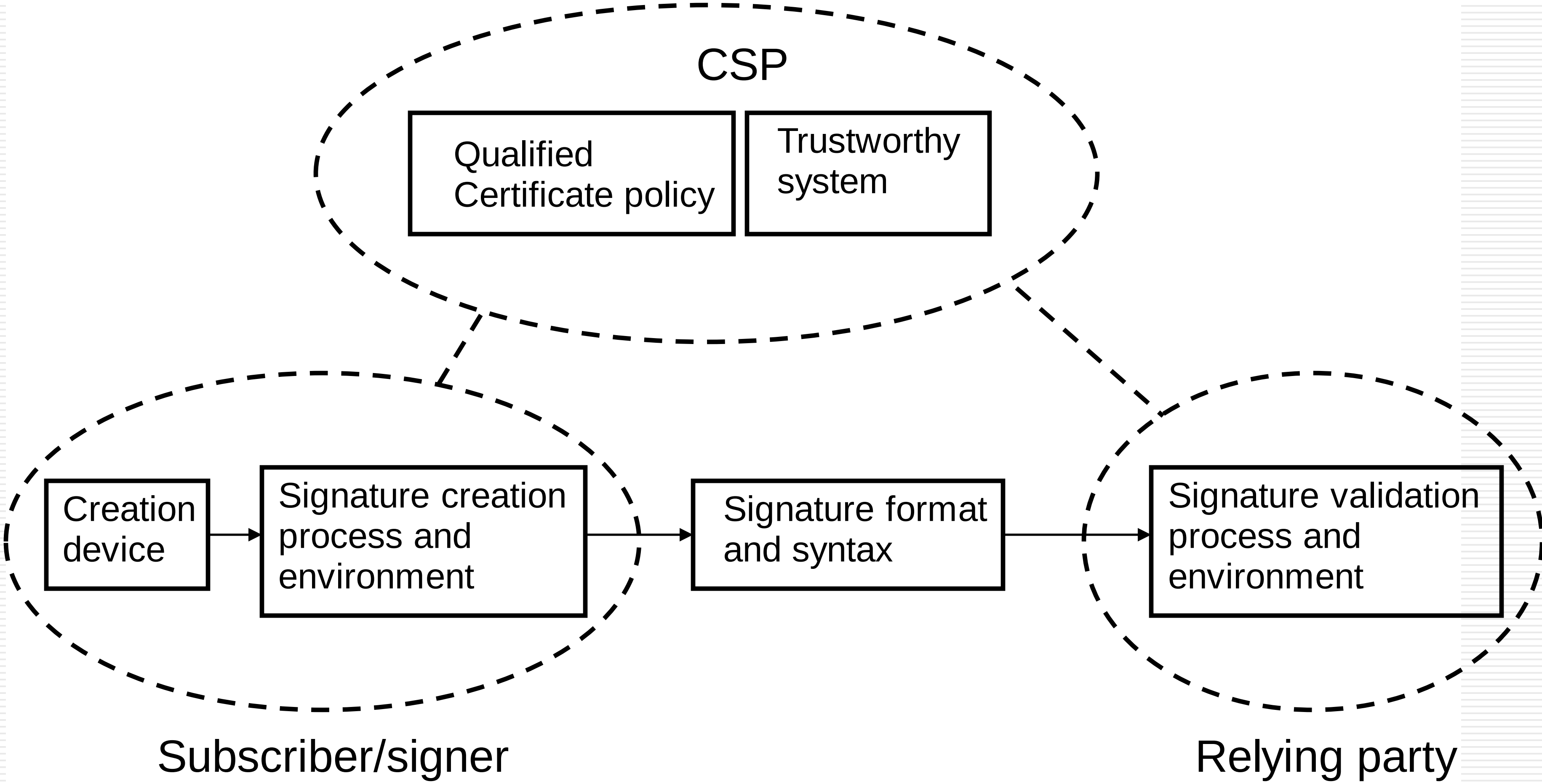
Proposed Classes of Electronic Signatures

Classes of signature:	**General electronic signature** as required in 5.2	**Qualified electronic signature -** as specified in 5.1 (Annex I, II, III)	**Enhanced electronic signature** (applicable to both general and qualified electronic signatures)
Level of legal certainty:	Can not be denied legal effect (art 5.2)	Same legal effect as hand-written signature (art 5.1)	Enhancement of technical evidence
Explanation:	Any electronic signature that is not a qualified electronic signature.	Minimum technical level required for the signer so that his electronic signature can be considered as legally equivalent with a hand-written signature.	Additional technical requirements for a verifier, such as time-stamping, but also for the signer, to enhance technical security and obtain protection against certain threats.

EESSI Objectives

- Analyse needs for standards in support of minimum essential legal requirements as stated by the Directive
- Assess available standards and current initiatives at national, European and international levels
- Set up and implement a Programme of Work, built on international co-operation

EESSI standards overview


CSP
Qualified Certificate policy
Trustworthy system
Creation device
Signature creation process and environment
Signature format and syntax
Signature validation process and environment
Subscriber/signer
Relying party

Review

- The meaning of authentication and identity
- Difference between user authentication and message authentication
- User authentication methods
- Message authentication
- Digital signatures and legislation