INF3510 Information Security
University of Oslo
Spring 2012

Lecture 7

User Authentication

Audun Jøsang

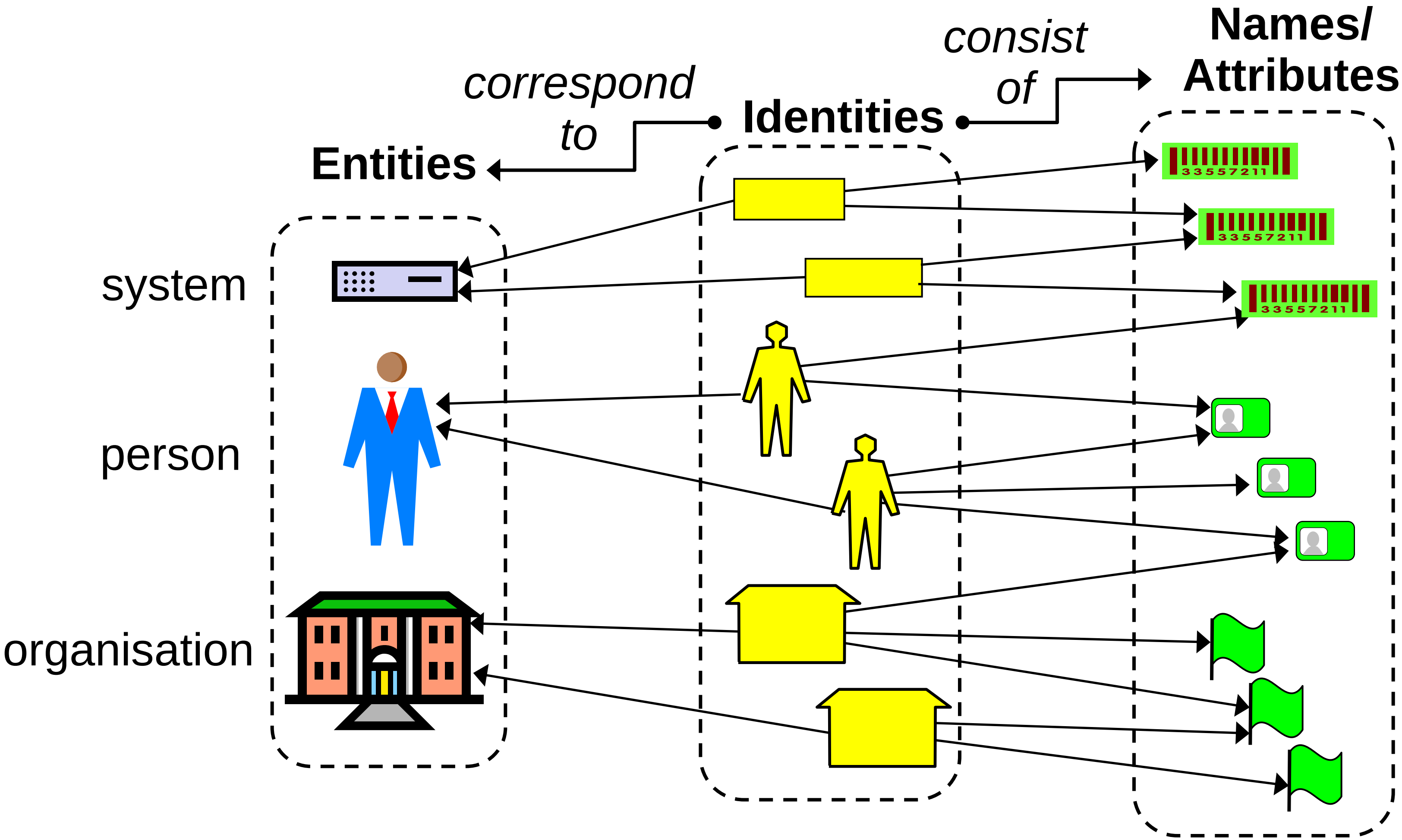
Outline

- Concepts related to authentication
  - Identity
  - User authentication vs. message authentication
- User Authentication
  - Knowledge-Based Authentication
    - Passwords
  - ID-Based Authentication
    - Biometrics
  - Object-Based Authentication
    - Tokens

Identity

- Etymology (original meaning of words)
  - *“identity” = “same one as last time”.*
- “First-time” authentication is not meaningful
  - because there is no “last time”
- Authentication requires a first time registration of identity in the form of a name within a domain
- Registration can be take two forms:
  - pre-authentication, from previous identity, e.g. passport
  - creation of new identity, e.g. New born baby

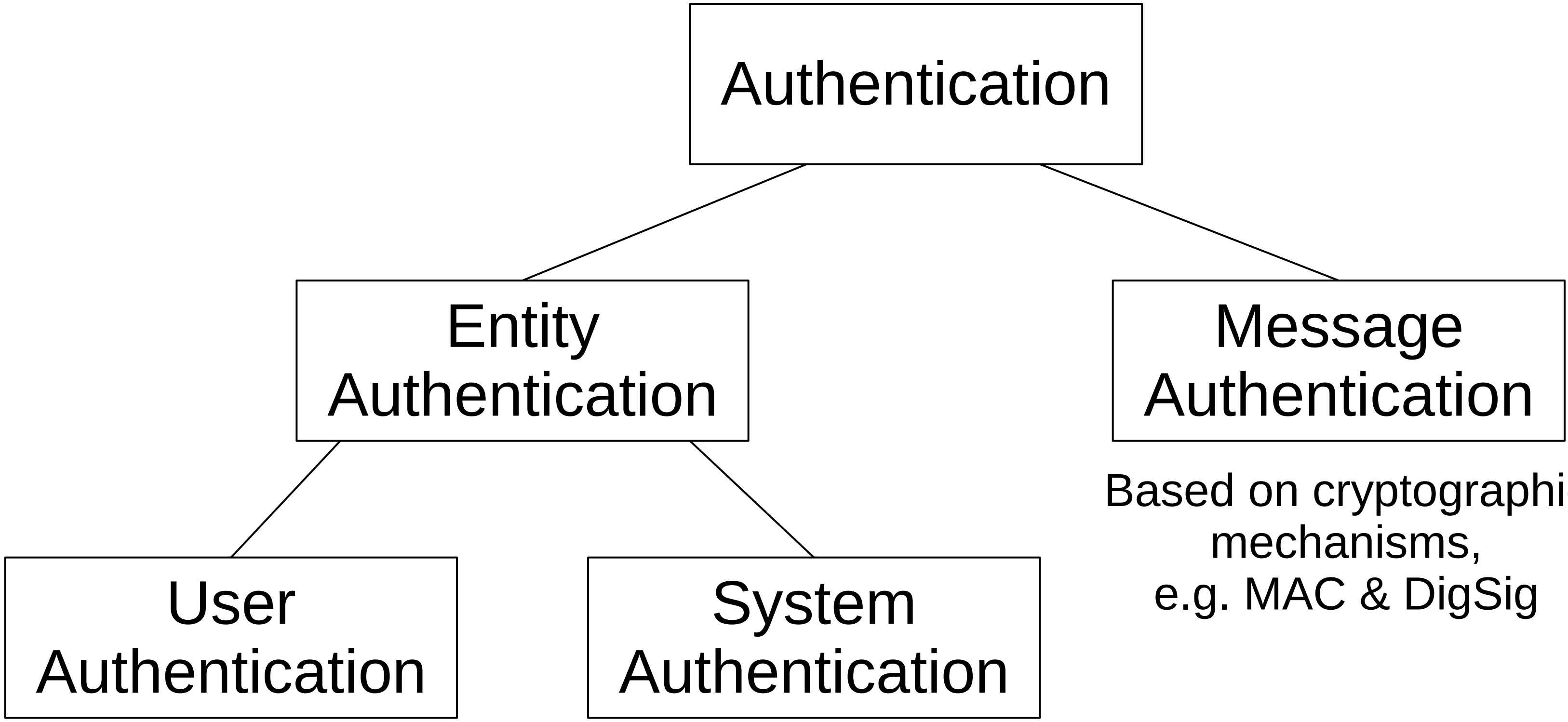
The Concept of Identity



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

Taxonomy of IT Security Authentication



Authentication

Entity Authentication

Message Authentication

Based on cryptographic mechanisms,
e.g. MAC & DigSig

User Authentication

Based on various types of credentials
e.g. passwords

System Authentication

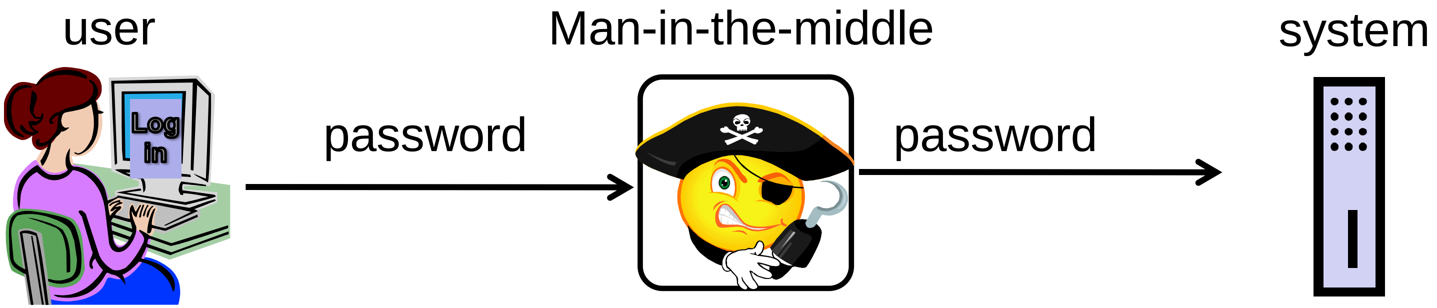
Based on cryptographic protocols
e.g. TLS & IPSec

Entity Authentication

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

Limitation of user authentication in sessions

- Applies to the start of a session (association) between a user and a system.
- Assumes e.g. that user operates 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



Message (Data Origin) 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

User Authentication

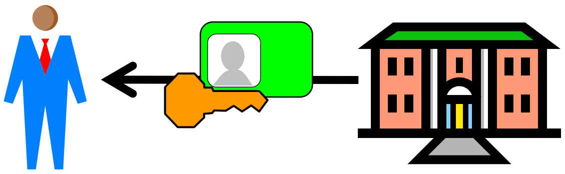
Stages of User Authentication

Registration phase (only once)

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

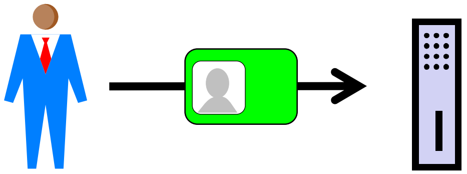
PASSPORT
United States of America

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

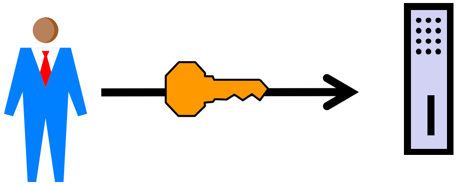


Authentication phase (multiple times)

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



4. Verification of identity
   - Proves Id with credential



User 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

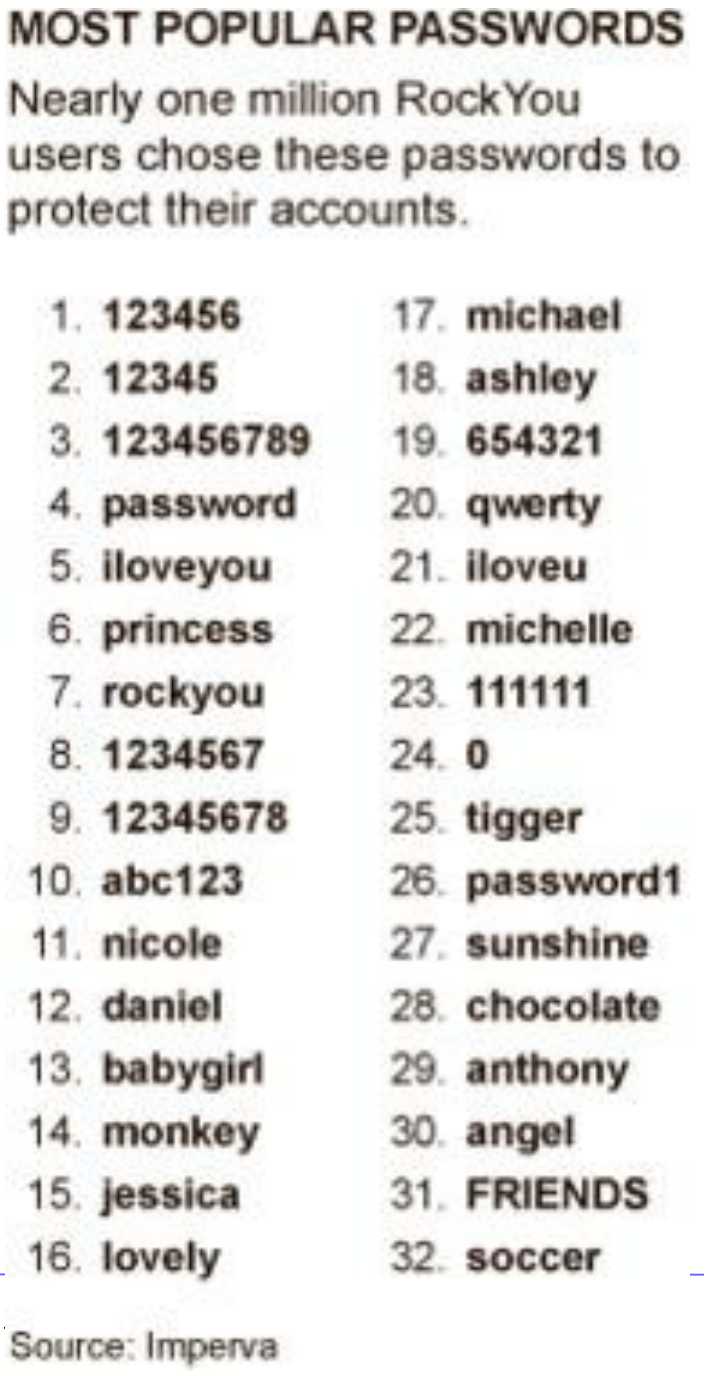
- Passwords are a simple and most-often-used authenticator.
  - Something the user knows
- Problems:
  - Easy to share (intentionally or not)
  - Can be forgotten
  - Often easy to guess
  - Can be written down (both god and bad)

Strategies for strong passwords

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

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**

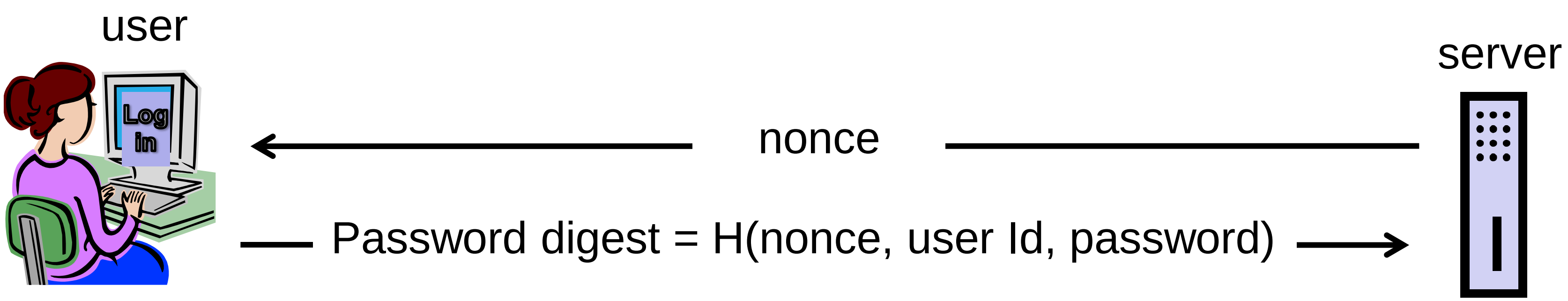
Source: Imperva

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

Digest Authentication: HTTP Digest

- A simple challenge response protocol specified in RFC 2069
- Server sends:
  - WWW-Authenticate = Digest
  - realm=“service domain”
  - nonce=“some random number”
- User specifies UserId and Password in browser window
- Browser produces a password digest from nonce, UserId and Password using a 1-way hash function (SHA-1….)
- Browser sends UserId and digest to server, that validates digest



user

server

nonce

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

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,
- 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
- Safety:
  - Safe environment might be needed

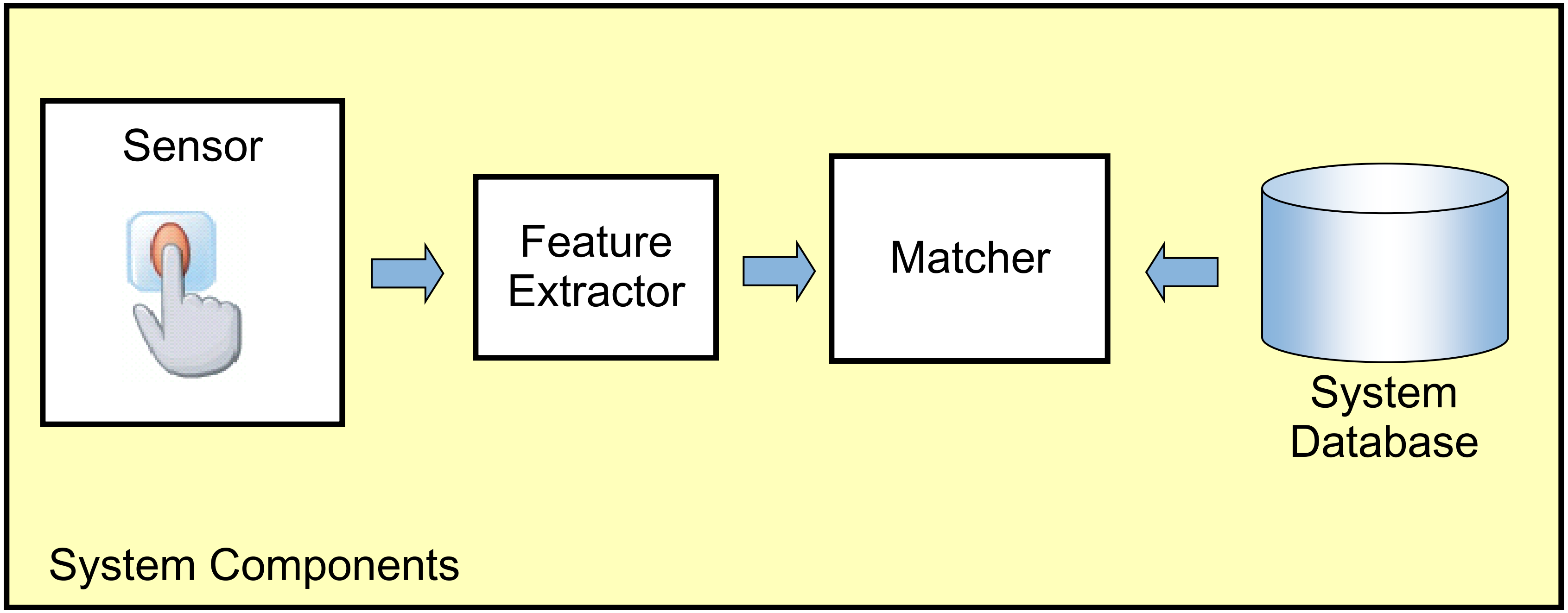
Biometrics Safety

- 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)

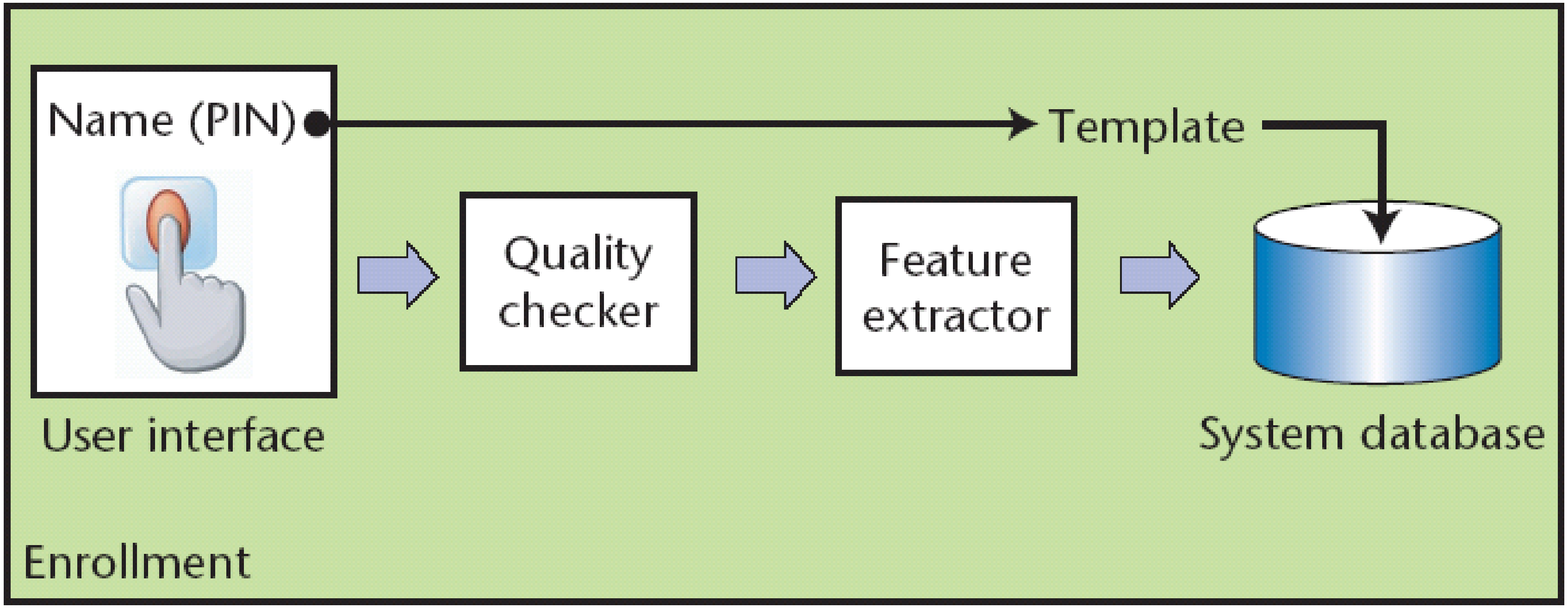
Biometrics: System components



Biometrics:
Modes of operation

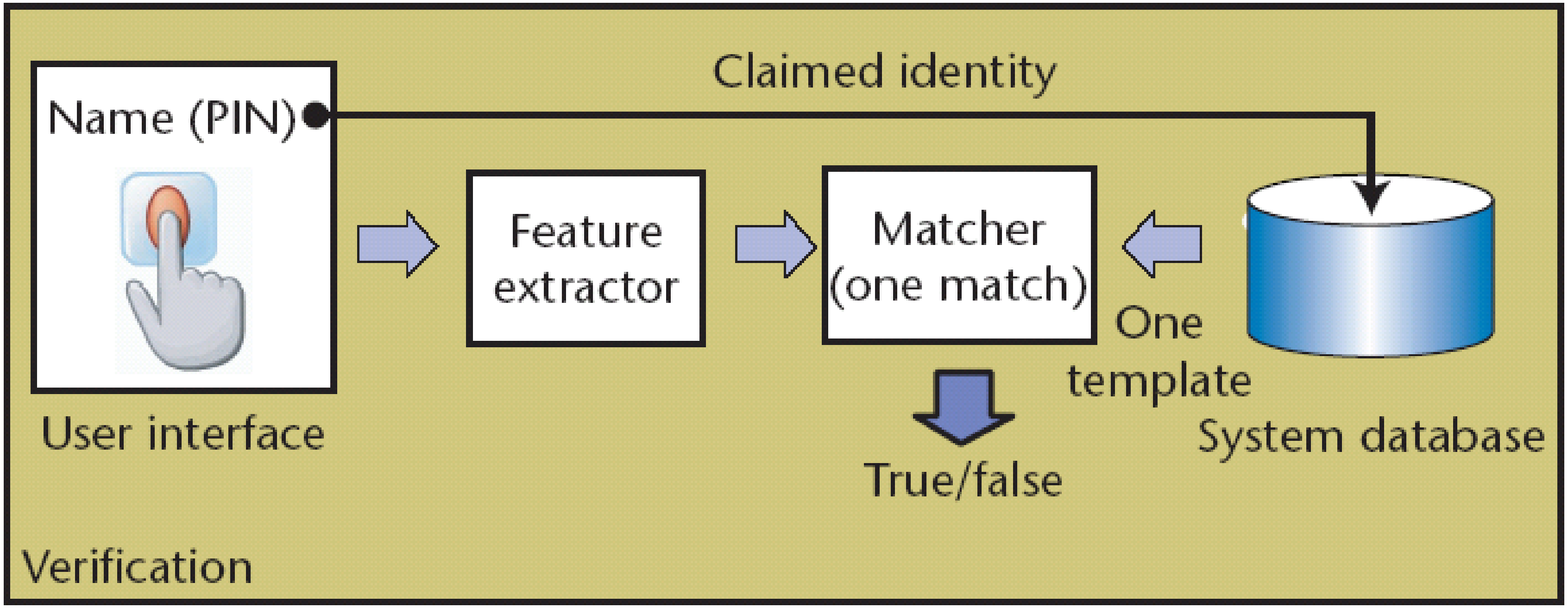
- Enrolment:
  - analog capture of the user’s biometric attribute.
  - processing of this captured data to develop a template of the user’s attribute which is stored for later use.
- Identification (1-to-many):
  - capture of a new biometric sample.
  - search the database of stored templates for a match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



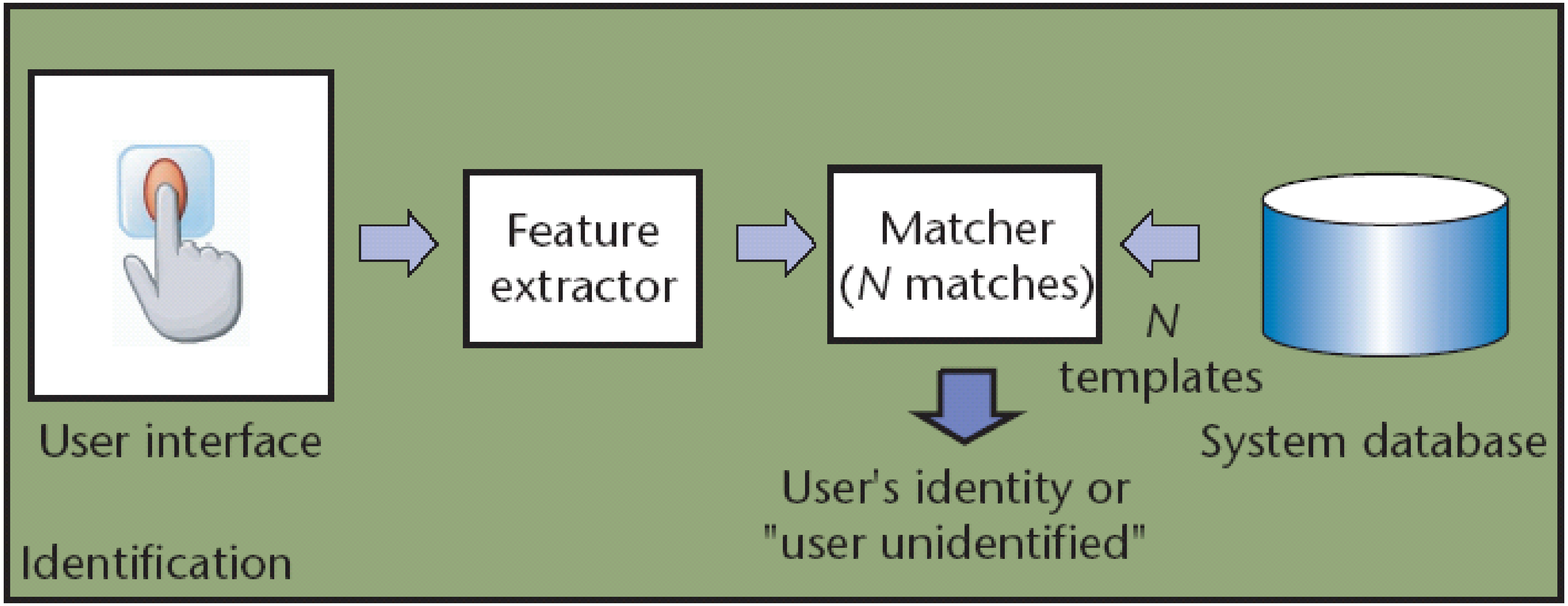
Biometric Recognition: Security and Privacy Concerns

Biometrics: Verification



Biometric Recognition: Security and Privacy Concerns

Biometrics: Identification



Biometric Recognition: Security and Privacy Concerns

Evaluating Biometrics:

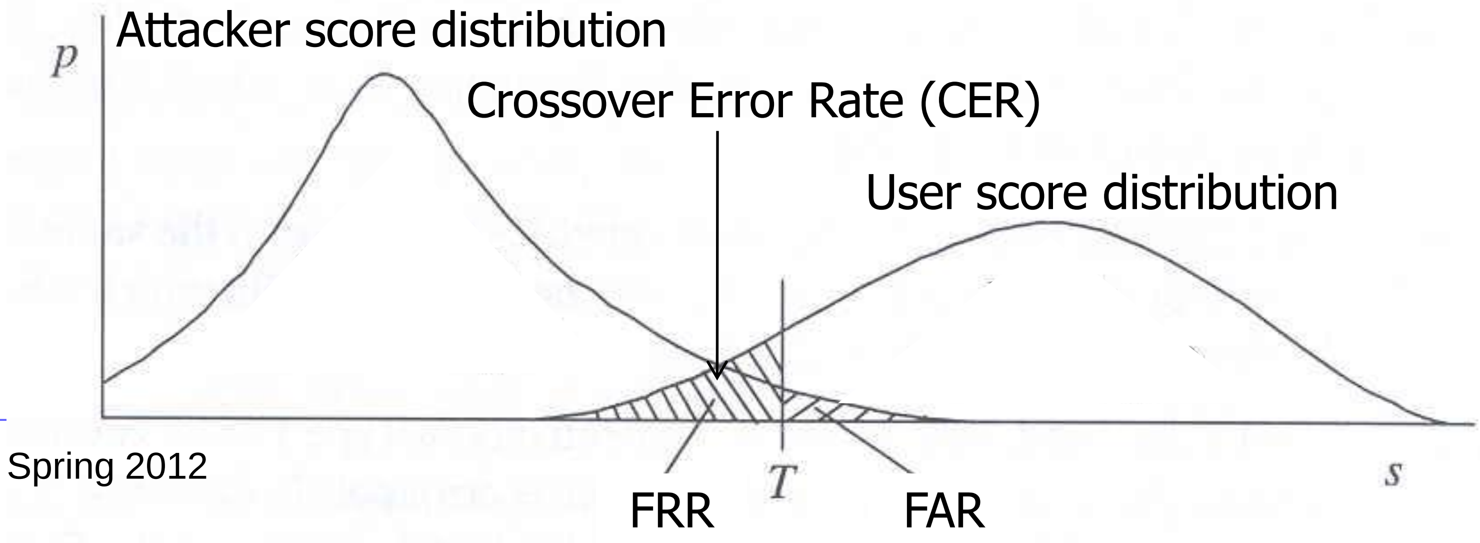
- Features captured during recognition are compared against the stored template
- Score *s* is derived from the comparison.
  - Better match leads to higher score.
- The system decision is tuned by threshold *T*:
  - pairs of biometric samples generating a score *s* where s ≥*T* are inferred as mate pairs (same person)
  - pairs of biometric samples generating a score *s* where *s* < *T* are inferred as non-mate pairs (different person)

Matching algorithm characteristics

- True positive
  - Legitimate user is accepted
- True negative
  - Attacker is rejected
- False positives → FAR (False Acceptance Rate)
  - Attackers are accepted
- False negatives → FRR (False Rejection Rate)
  - Legitimate users are rejected
- Tradeoff between FAR and FRR
  - FAR = (# accepted attackers) / (total # attackers)
  - FRR = (# rejected users) / (total # users)

Evaluating Biometrics: System Errors

- Comparing biometric sample produces score *s*
- Acceptance threshold *T* determines FAR (False Acceptance Rate) and FRR (False Rejection Rate)
  - If *T* is set low to make the system more tolerant to input variations and noise, then FAR increases.
  - On the other hand, if *T* is set high to make the system more secure, then FRR increases accordingly.
- Example score distributions of attackers and users:



Error Rates

- CER (Crossover Error Rate):
  - Size of overlapping areas of attacker score distribution and user score distribution
  - Small CER is good
- EER (Equal Error Rate):
  - Size of FAR (or FRR) when FAR = FRR
  - Small EER is good

- One of the measures is sufficient to judge the quality of a biometric system.

Object-Based Authentication

Something you have: Tokens

Synchronised OTP (One-Time-Password) Generator

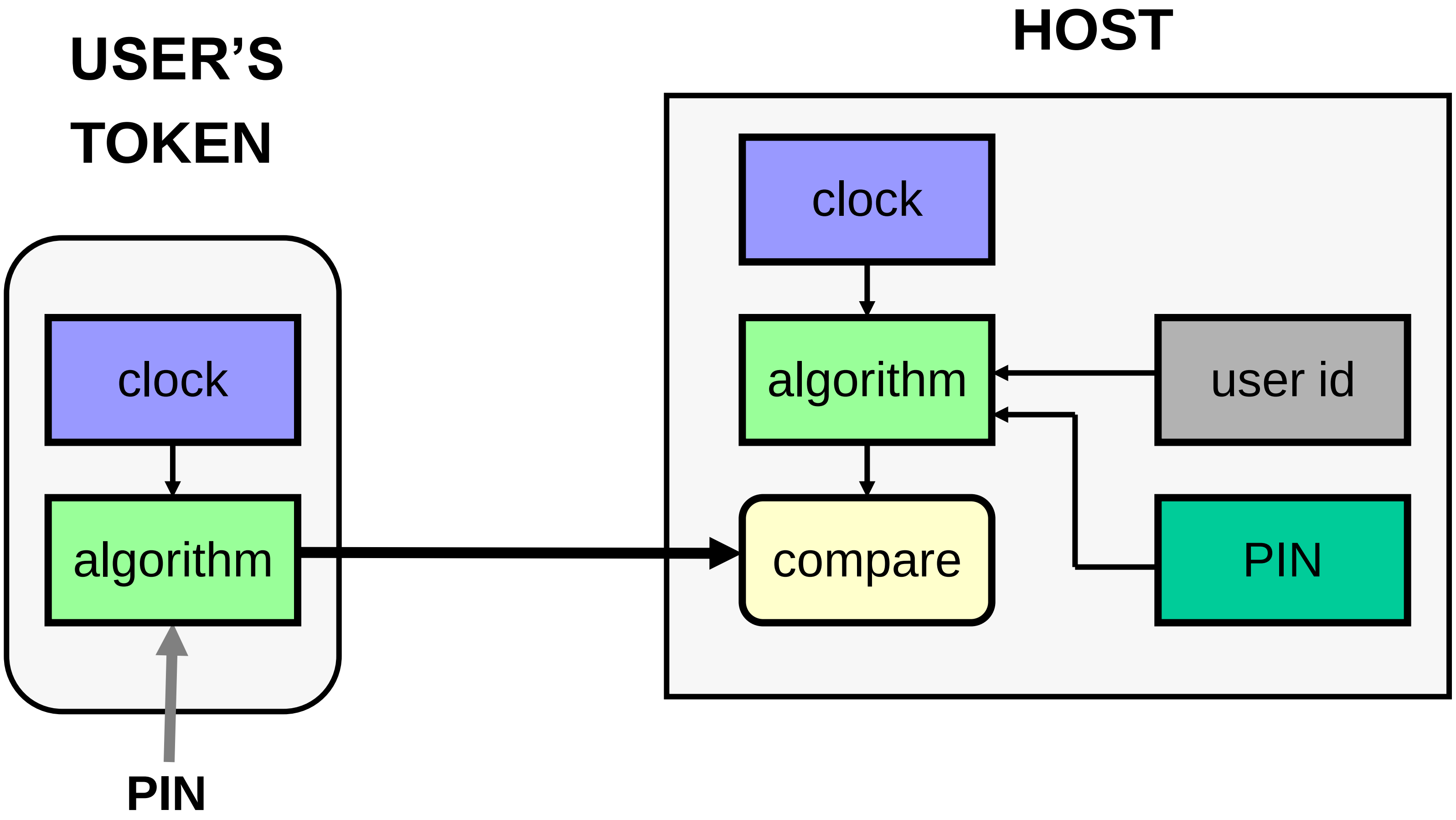
- Using a password only once significantly strengthens the security of the user authentication process.
- Synchronized password generators produce the same sequence of random passwords in a token and at the host system.
  - Is this ‘something you know’ or ‘something you have’?
- There are two general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

Diagram

Clock-based OTP Tokens: Operation



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

RSA SecurID SD600

RSA SecurID SID700

BankID OTP calculator with PIN

RSA SecurID SD200

BlackBerry with RSA SecurID software token

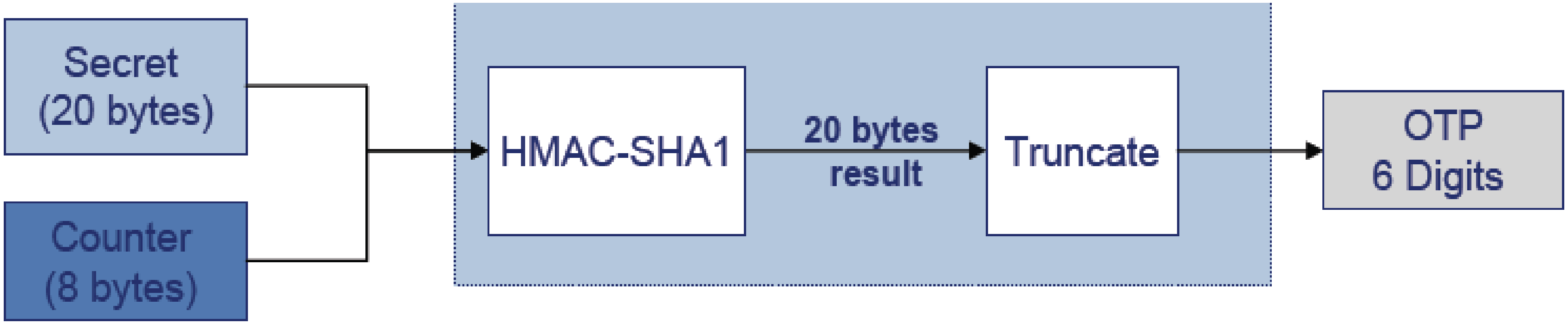
BankID OTP calculator without PIN

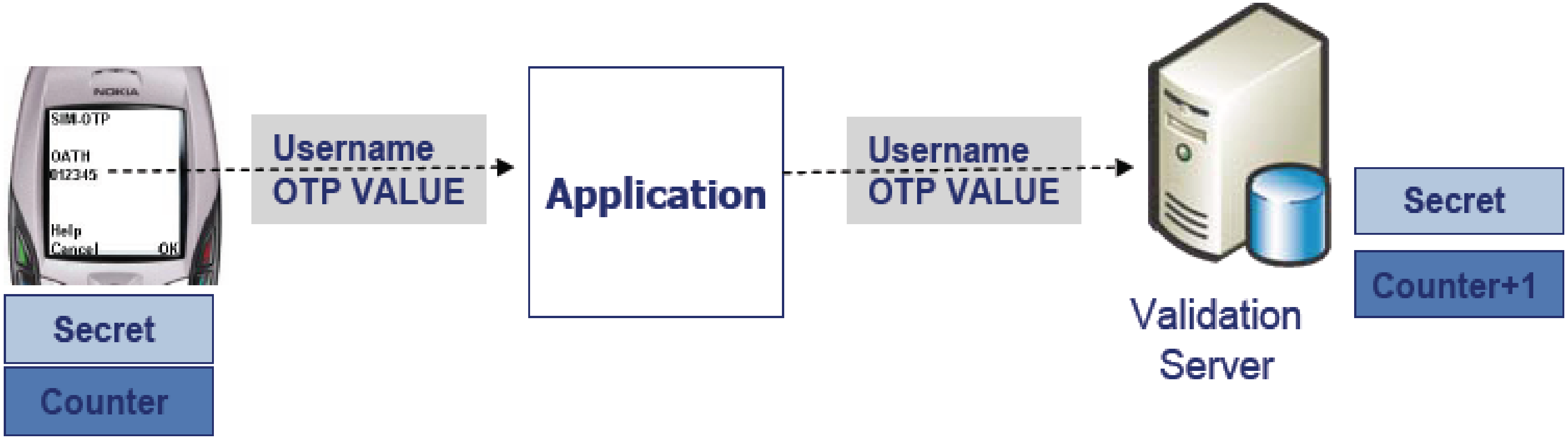
Counter-based OTP Tokens: Overview

- 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.

Reflex 530

Counter-based OTP Tokens: HOTP

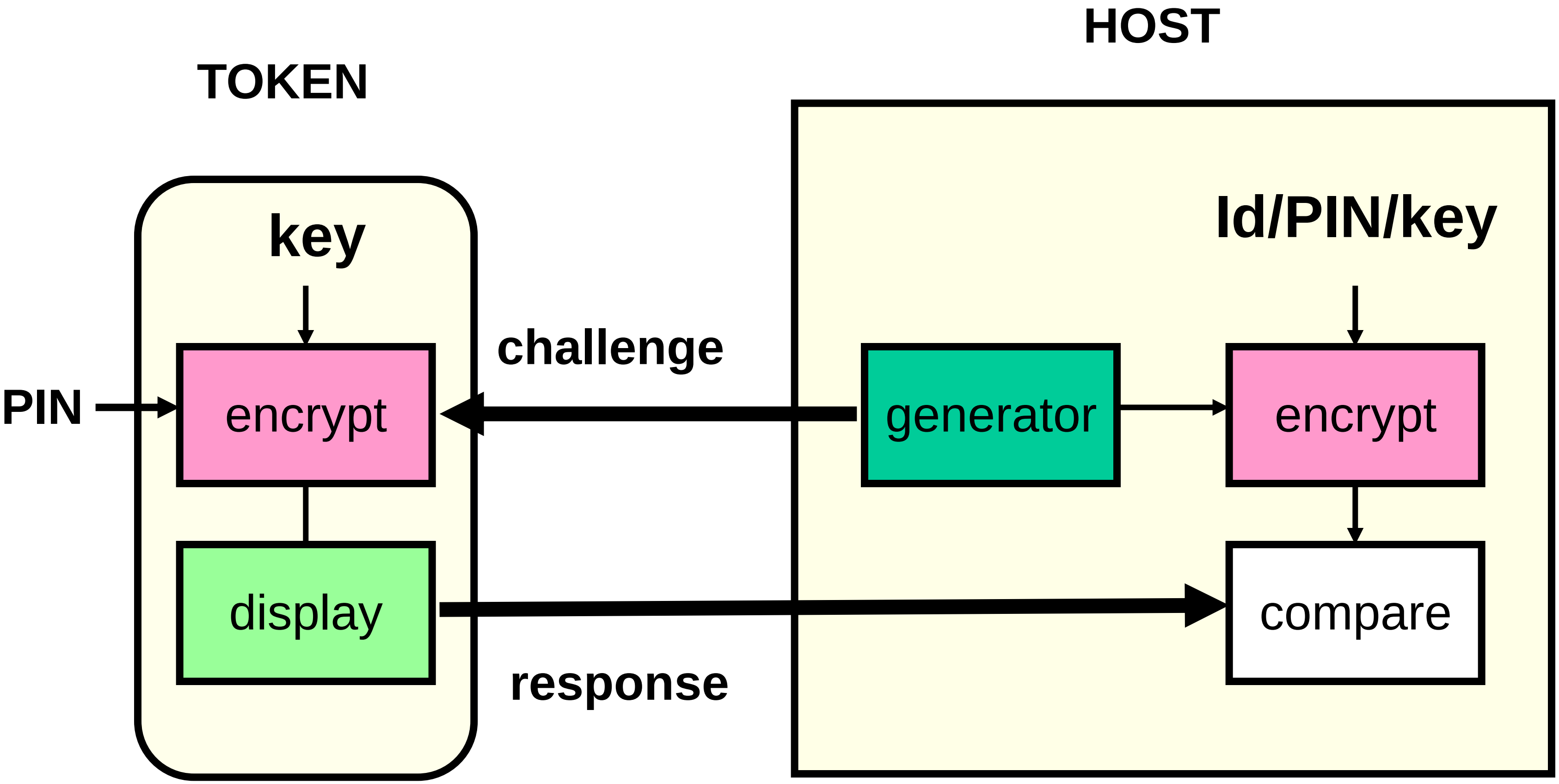




Token-based User Authentication: Challenge Response Systems

- 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

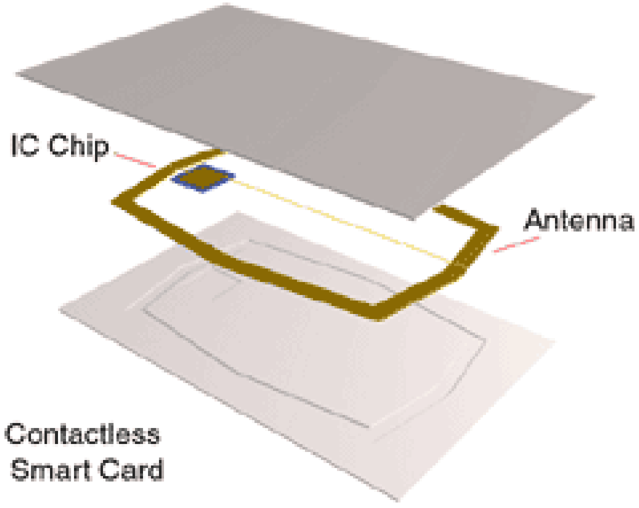
Token-based User authentication
Challenge Response Systems



Symmetric Case

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

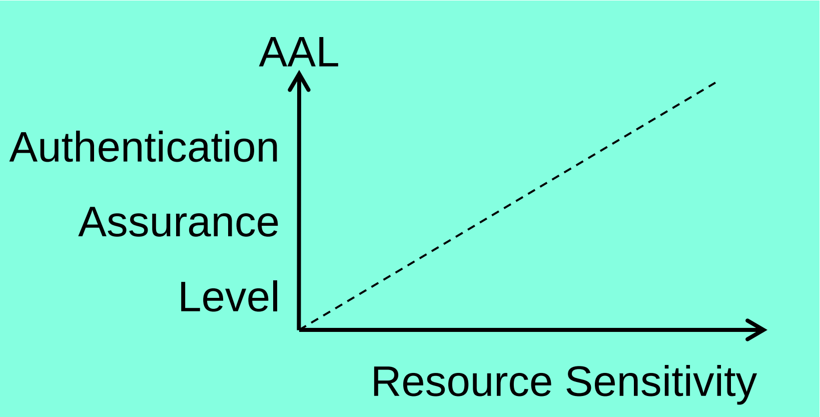


Authentication: Multi-factor

- 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

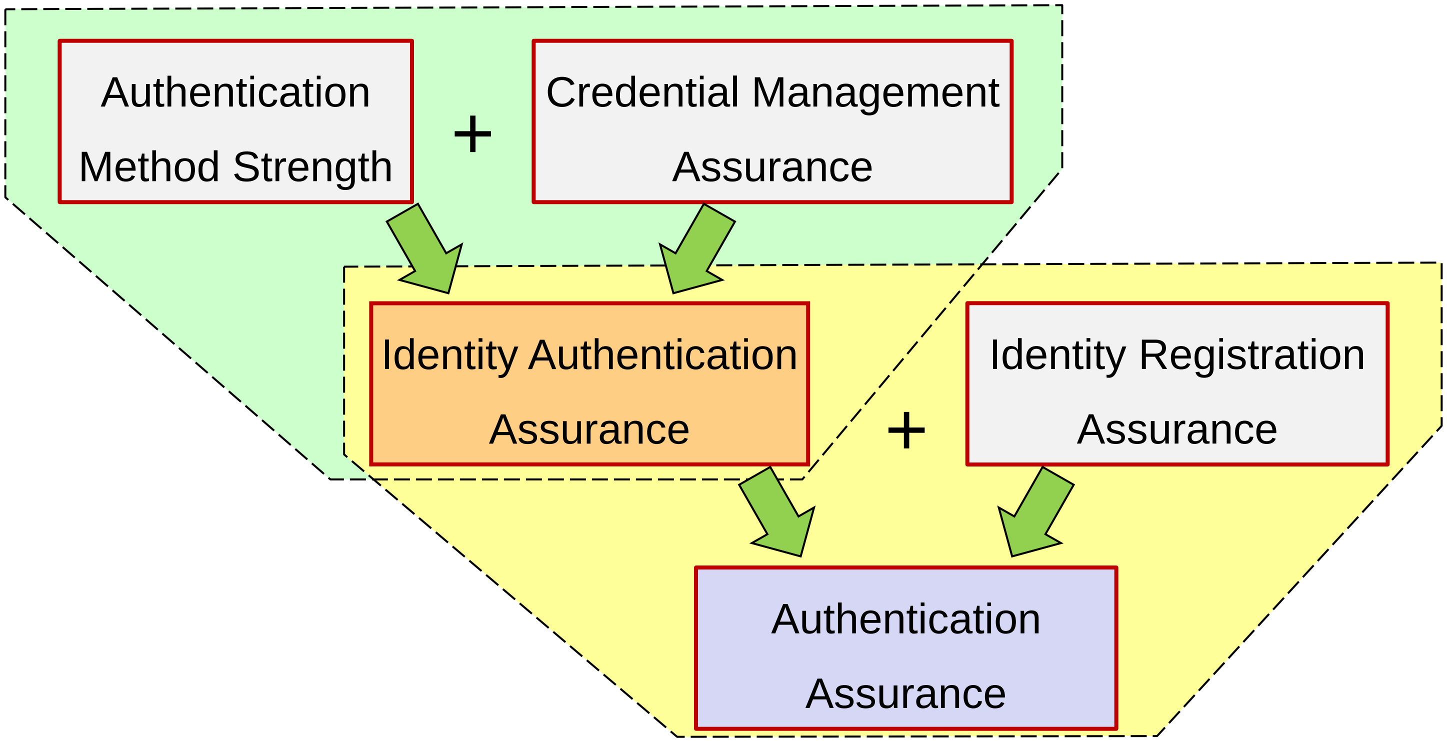


Why authentication frameworks?

- 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 Method Strength
+
Credential Management Assurance
Identity Authentication Assurance
+
Identity Registration Assurance
Authentication Assurance

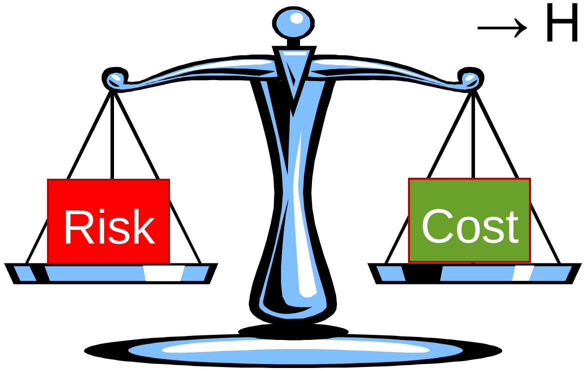
Authentication Assurance Requirement

- 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

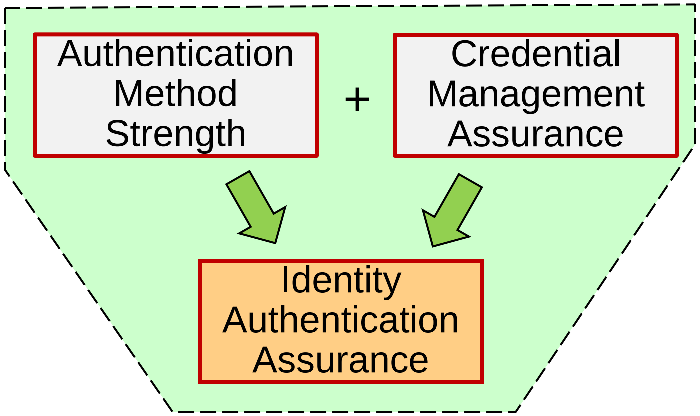
No Assurance	**Minimal Assurance**	**Low Assurance**	**Moderate Assurance**	**High Assurance**
Level 0	Level 1	Level 2	Level 3	Level 4
No registration of identity required	Minimal confidence in the identity assertion	Low confidence in the identity assertion	Moderate confidence in the identity assertion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

Example taken from Australian NeAF 2009

Identity Authentication Assurance Levels

Credential Management Assurance	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 Method Strength

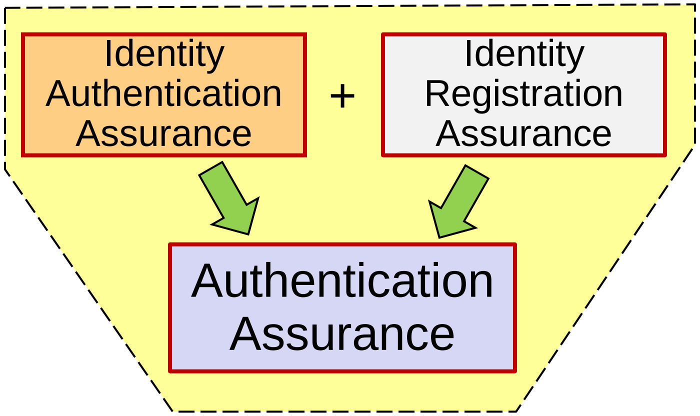

Authentication Method Strength
+
Credential Management Assurance
Identity Authentication Assurance

Authentication Assurance Levels

Identity Registration Assurance

	0	1	2	3	4
4		Minimal (1)	Low (2)	Moderate (3)	High (4)
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	None (0)	Pseudonymous Mininmal	Pseudonymous Low	Pseudonymous Moderate	Pseudonymous High

Identity Authentication Assurance



Identity Authentication Assurance + Identity Registration Assurance

Authentication Assurance

Comparison of Assurance Levels

<table>
<tr><th></th><th colspan="8">Assurance Levels</th></tr>
<tr><td><b>IDABC (EU)</b></td><td>N/A</td><td colspan="2">Minimal
(1)</td><td colspan="2">Low
(2)</td><td colspan="2">Substantial
(3)</td><td>High
(4)</td></tr>
<tr><td><b>NeAF (Au)</b></td><td>None
(0)</td><td colspan="2">Minimal
(1)</td><td colspan="2">Low
(2)</td><td colspan="2">Moderate
(3)</td><td>High
(4)</td></tr>
<tr><td><b>NIST (US)</b>
<b>FANR (Norw.)</b></td><td colspan="3">Little or None
(1)</td><td colspan="2">Some
(2)</td><td colspan="2">High
(3)</td><td>Very High
(4)</td></tr>
<tr><td><b>UKOnline</b></td><td colspan="2">Minimal
(0)</td><td colspan="2">Minor
(1)</td><td colspan="2">Significant
(2)</td><td colspan="2">Substantial
(3)</td></tr>
</table>

- IDABC: Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens.
- NeAF: National e-Authentication framework
- NIST: National Institute of Standards and Technology
- FANR: Framework for Authentication and Digital Signatures (Rammeverk for Autentisering og Uavviselighet)

Authentication assurance options Level 1 (FANR 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 (FANR 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 (FANR 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 (FANR 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.

Provides very high authentication assurance.

Risk Analysis for Authentication

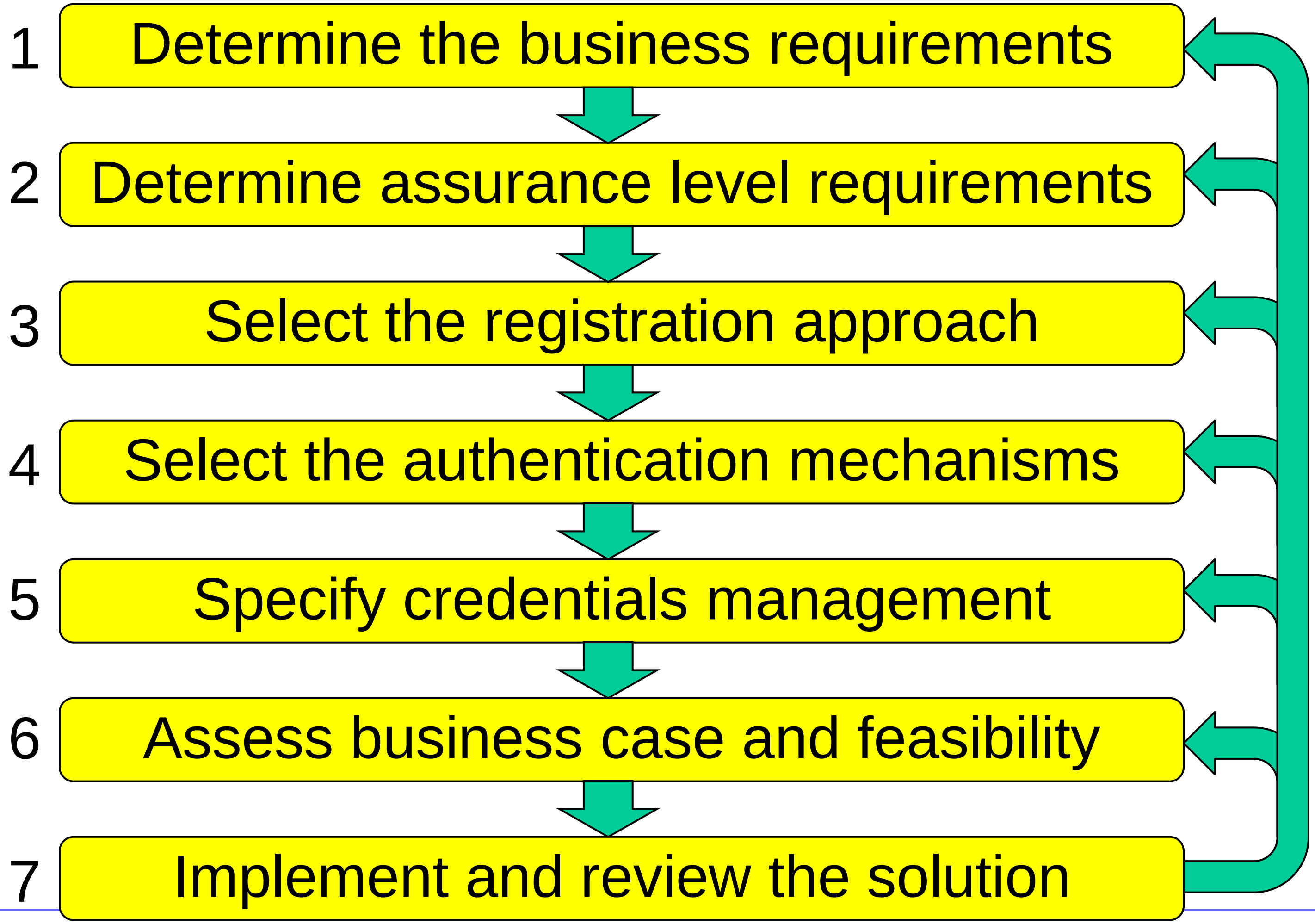
Determines required Authentication Assurance Level

		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)

Required AAL

Example: NeAF Australia

Steps of an Authentication Framework



1 Determine the business requirements

2 Determine assurance level requirements

3 Select the registration approach

4 Select the authentication mechanisms

5 Specify credentials management

6 Assess business case and feasibility

7 Implement and review the solution

End of lecture