Government Digital Delivery Agency
Te Pūnaha Matihiko

Introduction to Identification Management

Joanne Knight and Daniel Anderson
Identification Consultants

12 May 2026
Privacy Week 2026

Introduction to Identification Management

- What is Identification Management
- Identification Management and integrity
- Identification Standards for New Zealand
- Guidance
- Training, clinics and resources
- Pātai / questions

What is Identification Management

It’s about managing processes

- Verifying information
- Connecting information to Entities (e.g. people)
- Connecting information and Entities to reusable Authenticators (e.g. passwords, keys, biometrics)

Identification Management applies when you enrol Entities and throughout the lifetime of their relationship with you.

Identification Management:

- covers entities other than people — ***Any entity,***
- is product neutral, and — ***any information,***
- is channel agnostic — ***any channel!***

Identification Fundamentals

Organisations (“*relying parties*”)

can get the

right information (“*attributes*”)

about the

right subjects (“*bound entities*”)

and can

recognise (“*authenticate*”)

them when they return

Identity concepts

Two concepts:

Identity (security): The (minimum) number of attributes that allow a record/account to be unique from all others in a context

- Information security view
- Centres on a small set of identifiers
- Been around for 40-ish years

Identity (origin): The characteristics and qualities of being a specific person or thing; individuality

- Business and wider view
- Centres on the person/thing and their information
- Since sentience began

Why Identification Management is important

To prevent identity theft!

Identity theft:

- results in fraud
- costs people and organisation money and reputation
- causes loss of privacy and security
- is detrimental for you and your customers.

Good identification management practices contribute to good business processes for effective decision-making and risk management.

Identification Management works with privacy and security to protect information, not to replace or compete with them.

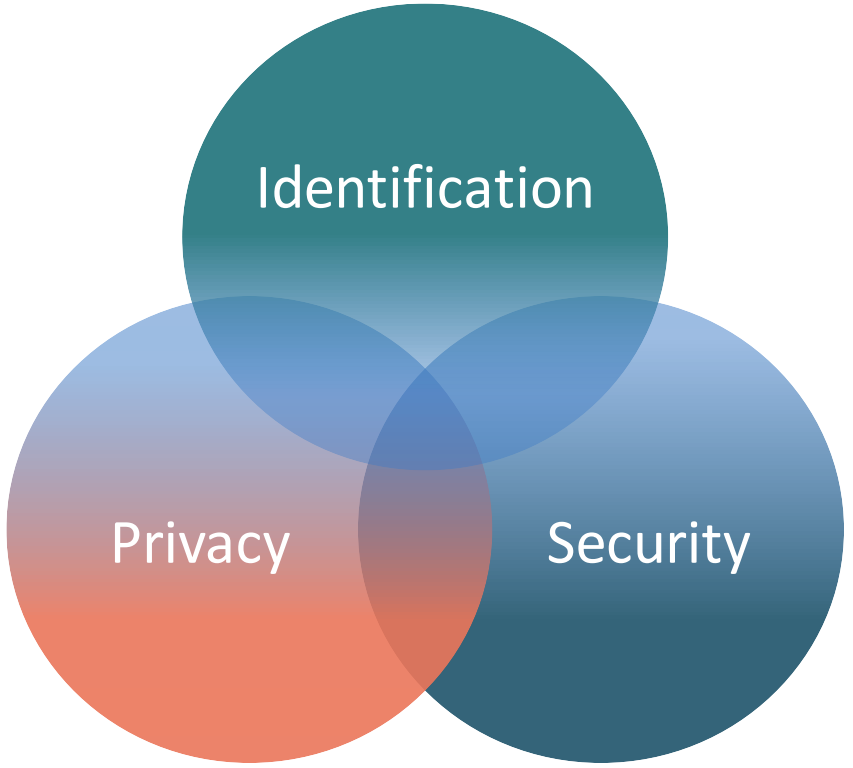
Separate but related practices

Security is great for preventing technical attacks, but not so good with human behaviours for account take-over.

Privacy is great about personal information, but not for processes for Entities that aren't natural persons.

Identification overlaps these two practices, as it is an enabler for both and fills some important gaps.

Poor practices in any of these areas result in bad outcomes for people and organisations.



Common presumptions

1. Officially-identifying people will stop them behaving in a bad way.

2. The more information collected, the more likely it is the right person.

3. Officially registered name and date of birth are the only way to verify eligibility and match customers.

4. Over-collecting information means we must have the right person.

5. Knowing information means owning the account.

6. Everyone has the same definition of ‘identity’.

Common mistakes

“Identity” is the ‘purpose’ for collection, and is the ‘solution’ to prevent fraud, integrate services, and make service delivery more efficient.

Privacy breaches are more likely to happen because of over-collection while not addressing the underlying issues!

Focusing on ‘digital’ at the exclusion of other channels.

Identification is a core competency for all channels just like security and architecture. Fraudsters exploit ignored channels with increasing capability.

Trying to solve identification needs with products and service-specific projects.

End up with either a bespoke solution you can’t use elsewhere, or identification processes are de-scoped from the project or put into the backlog.

Identification Management and integrity

Why an identification approach is important

To prevent **identity theft:**

Current approaches don't stop people using some else's information as their own.

Good identification practices increase security, protect privacy, and prevent fraud.

To focus on the **right information:**

Essential to determine eligibility, capability, and permissions.

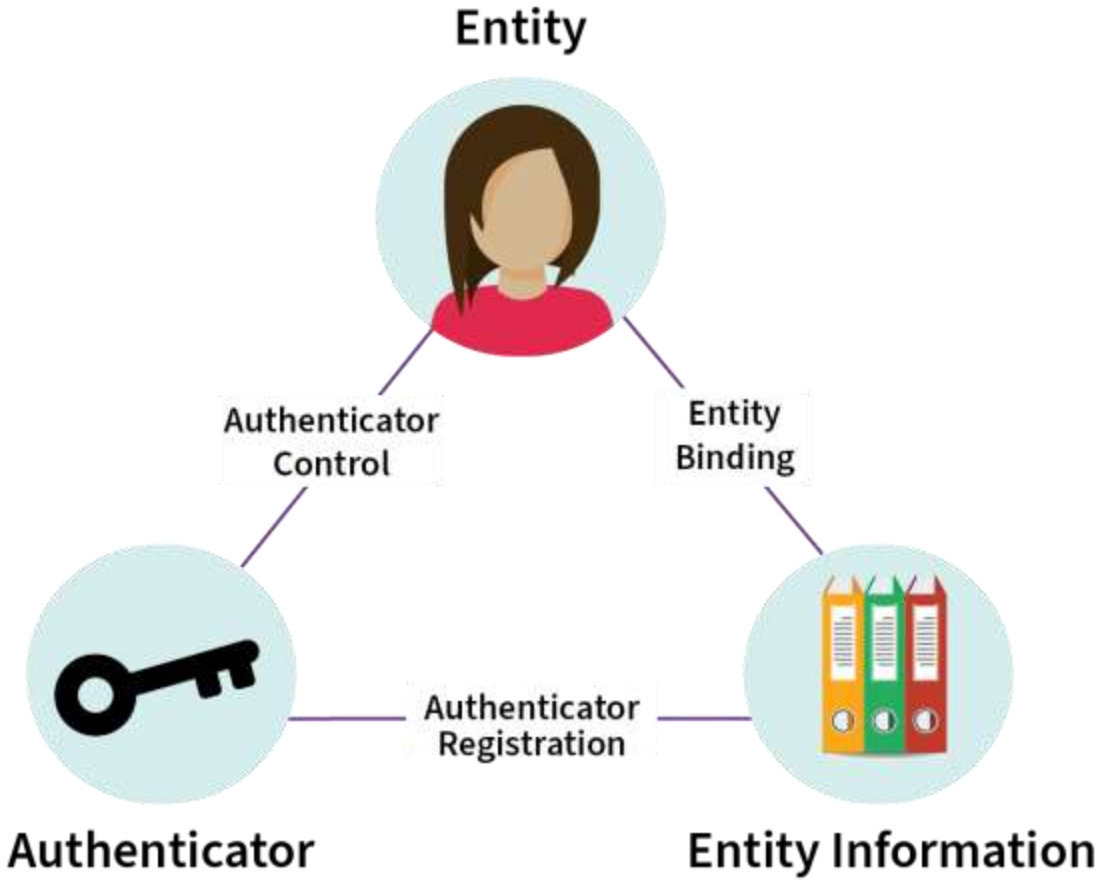
To mitigate **identification risk:**

1. Incorrect information is provided for a service or transaction.
2. An entity is incorrectly linked to or associated with the information and/or authenticator used in a service or transaction.

Integrity: the Triangle

Maintaining the integrity of this triangle means you know the right person is returning.

When this triangle is broken, identity fraud happens.



Robustness: Levels of Assurance

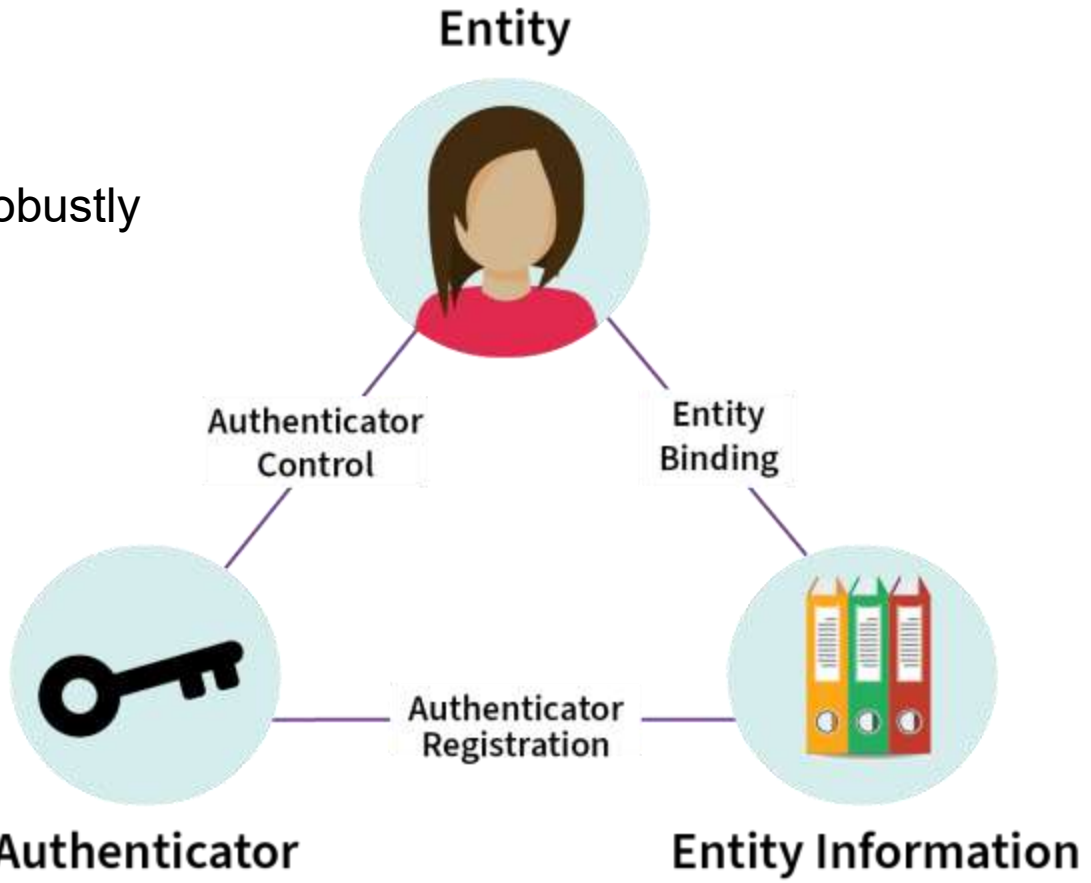
Business processes need to define and measure how robustly they:

- verify information about an individual
- bind this information to the individual
- connect these to reusable Authenticators.

Each of these can have different levels of assurance!

Levels of Assurance are expressed as a number:

1 is low robustness, scaled up to **4** for high robustness.



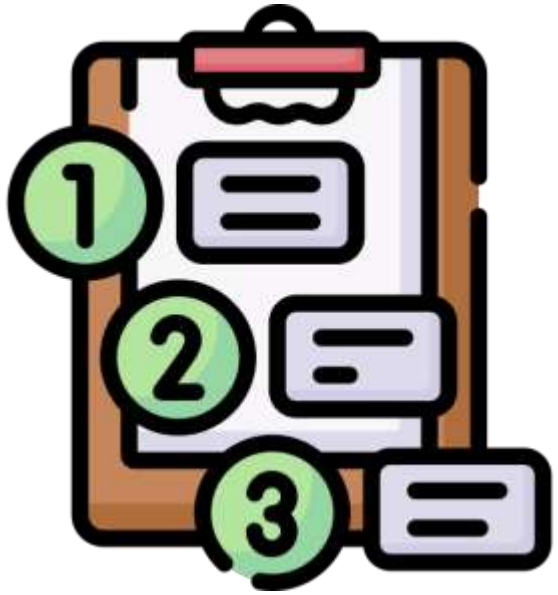
Identification Standards for New Zealand

What are Standards?

Standards describe the best way to do something. They are testable and repeatable.

The best way to do identification management is to follow a standard.

Standards bring consistency and rigour to common processes.



Identification Standards for New Zealand

There are many related standards around the world, but they are often:

- digital focused
- based on National ID
- inflexible, or designed for a very specific audience or requirement
- tied to technology and date easily.

The **New Zealand Identification Standards** are:

- risk-based
- not focused on universal identifiers
- build in privacy and security from the start
- channel neutral
- usable with other approaches like self-sovereign, decentralised identifiers, verifiable credentials, etc.
- written for the New Zealand context but also work globally.

Relying Party Standards

Information Assurance Standard:

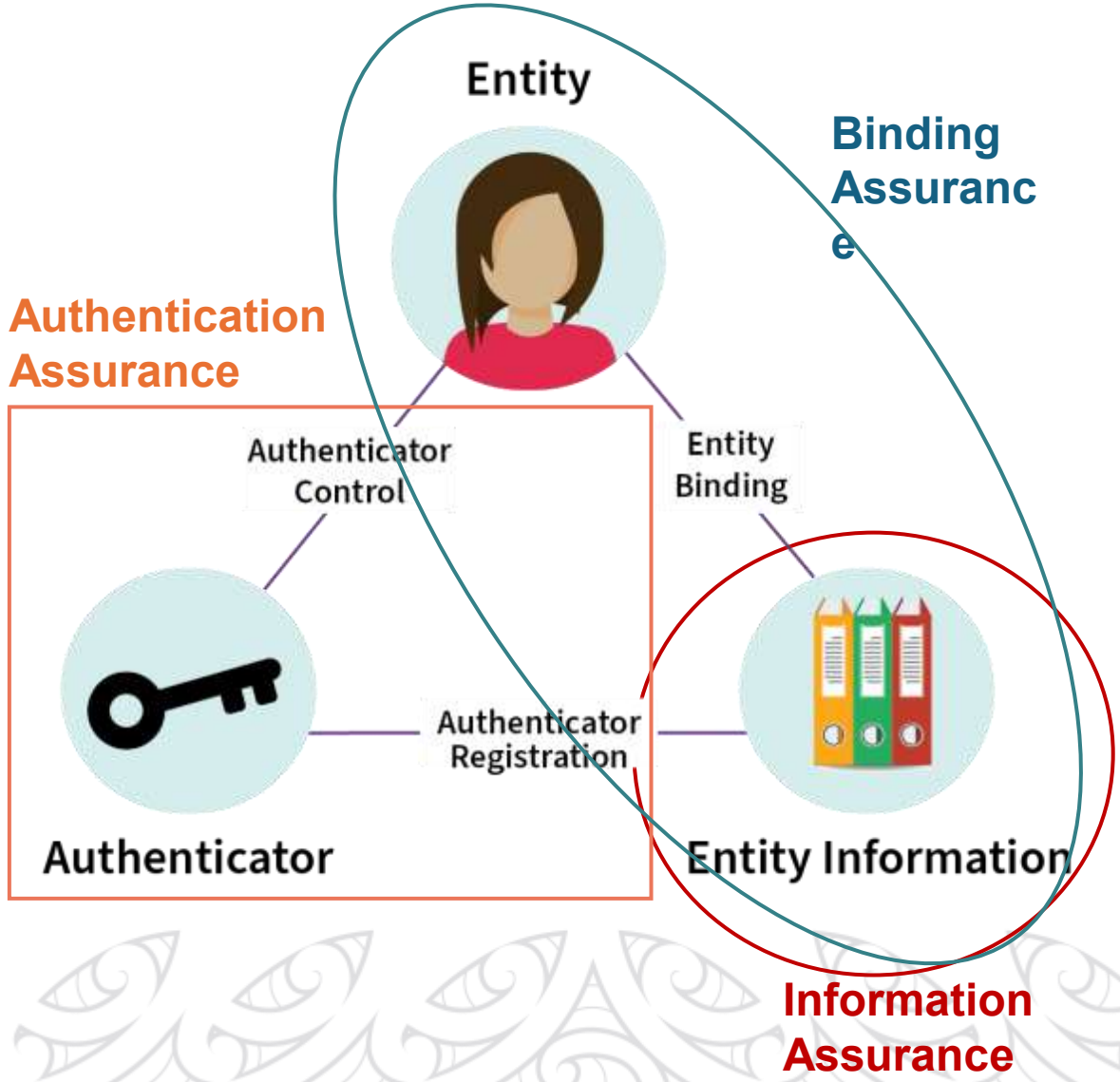
Levels of assurance for the quality and accuracy of Entity Information.

Binding Assurance Standard:

Levels of assurance for binding the Information to the Entity.

Authentication Assurance Standard:

Levels of assurance for ensuring an Authenticator remains solely in control of its holder.



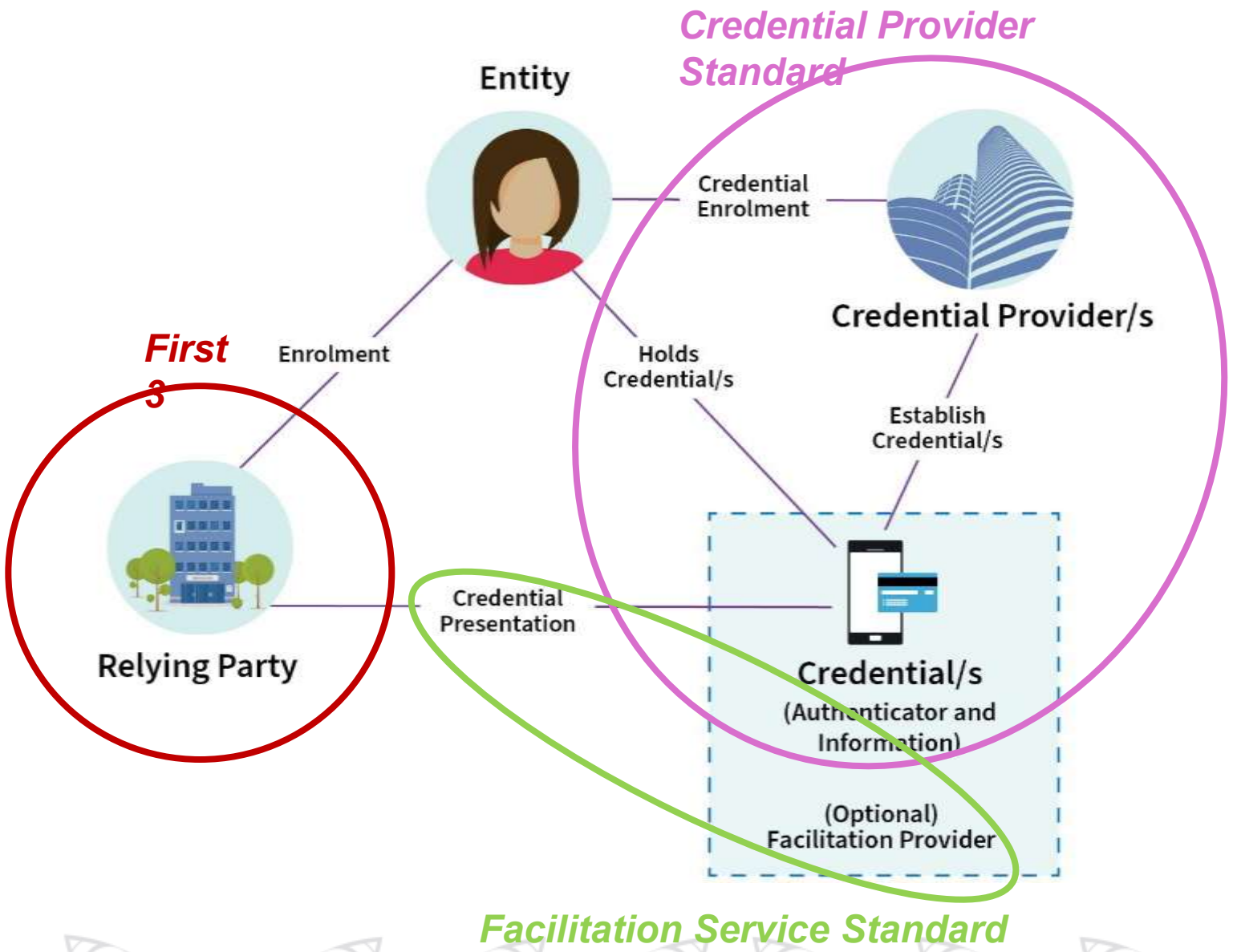
A bigger picture: Federation

Credential Service Standard:

Additional steps for Credential Providers to maintain the integrity, security and privacy of a credential.

Facilitation Service Standard:

Additional steps for Facilitation Providers establishing facilitation mechanisms (e.g. digital wallets) and presenting Credentials.



How the Identification Standards work

Each Standard covers a specific **Scope.**

Example: Information Assurance applies whenever information related to an Entity is collected and stored (whether during enrolment or a subsequent transaction).

Standards are made up of requirements called **Objectives** that describe *what you are trying to achieve*. Each Objective represents a threat to be mitigated.

Example: Information Assurance Objective 2: Information is protected

Each Objective is made up of **Controls** that describe *how to mitigate* the threat.

Example: IA2.02: The Relying Party MUST have a justifiable need for every piece of information it collects.

The higher the Level of Assurance you want to meet, the more the Control may require you to do.

Identification Standards and the IPPs

Objectives and their Controls deliver many of the Information Privacy Principles. For example:

Control	IPP or expectation
IA3.03: The Relying Party verifies each piece of information using evidence at the established level of information assurance.	Principle 8 – Accuracy of personal information
FA3.01: The Credential Provider MUST reduce the ability for Relying Parties to correlate holders by not including the holder's unique Entity Information identifier as part of a Credential.	Principle 13 - Unique identifiers
AA2.03: The Relying Party limits the ability to share an Authenticator by implementing 2 different factor types. • Level 1 & 2: does not apply • Level 3: must do it unless a biometric factor is used • Level 4: must do it and a biometric factor has to be 1 of the factors	OPC expectation that 2FA be implemented

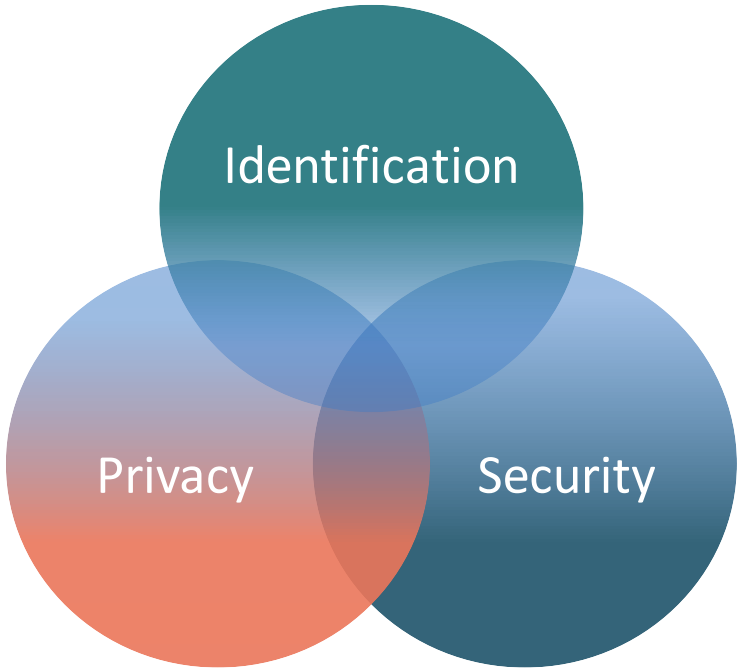
Identification and privacy both try to manage risk

Privacy by Design requires Privacy Impact Assessments to assess privacy risk and what you need to do to control it. Privacy risks in PIAs are often based around the 13 Information Privacy Principles.

Identification Management assesses risk by looking at the bigger picture with business processes at the core.

You only know how to manage your risk if you measure it first!

As privacy, security and identification overlap, risks in one space may be controlled by another.



Digital Identity Services Trust Framework

The Identification Standards are for public and private sector use.

They are **mandatory** if you are seeking Digital Identity Services Trust Framework accreditation.

Accredited digital identity service providers have proven they meet, and continue to meet, the standards for using, storing and sharing personal and organisational information.

Accredited services are listed in the Trust Framework Register.

Learn more at: https://www.dia.govt.nz/Trust-Framework

Guidance

Guidance

Each of the Identification Standards has its own implementation guide.

We also have guidance on:

- Assessing identification risk
- Using documents as evidence
- Authenticator types
- Counter fraud techniques
- Derived information and other calculated values (and for age assurance)
- Authority to act for another Entity

Assessing identification risk

To determine if your service or product has identification risk…

1. Can anyone receive money (e.g. benefits, grant, debt)?
2. Can anyone receive other benefits (e.g. access to a secure area)?
3. Is information about a person being collected and stored?
4. Can the service release personal or sensitive information?
5. Can the service issue a document or data source that can be used as evidence of identification?

This guidance helps outline the four types of controls - preventative, corrective, detective and disincentive - that can help manage your identification risk.

Risk measurement tools are also available to assess your identification risks.

Using documents as evidence

This guide provides information about the 3 types of document fraud:

1. Genuine document with the wrong owner
2. Genuine document that has been altered
3. Fake document

It also explains how to treat expired documents. Using expired documents does not mean the information in it has expired – but you may need other documents to help manage your risk.

This guide also warns against the use of photocopies, even when verified.

Authenticator types

There are 3 types of authentication factors:

- **Something you know** — challenges based on information known (e.g. password, PIN, security question).
- **Something you have** — challenges based on possession of an object (e.g. token, mobile phone, chip card)
- **Something you are** — challenges based on characteristics, biological or behavioural (e.g. face, fingerprint, voice, gait)

This guide describes each factor and its strengths and weaknesses for the channel they are used in.

It also explains what multi-factor authentication (MFA) is, where challenges and responses are needed in 2 or more of these 3 types.

MFA isn't:

- two factors of the same type – e.g. two passwords
- a user name and a password!

Counter fraud techniques

There's no one-size-fits-all approach for identification processes. These counter-fraud techniques are how to apply additional steps to increase your system's integrity:

- **Managing coercion and collusion:** in-person processes and segregating duties
- **Entities with limited evidence:** how to help children, refugees, and non-human Entities
- **Weak evidence quality:** verifying documents with issuers and gather additional evidence
- **De-duplication of Entity information:** collecting unchangeable values & unique identifiers
- **Counter fraud techniques for binding:** death checks, Trusted Referees, Entity use over time

- And much more……

Calculated information and age assurance

Values can be:

- **Derived:** directly calculated from one or more values
  - Example: calculating age from a date of birth
- **Inferred:** an assumption based on information
  - Example: a person with a credit card must be over 18 years old
- **Estimated:** statistical analysis from information.
  - Example: a social media account that has a consistent history of watching popular video game and toy videos may belong to a child

Authority to act for another Entity

Authorities to act are relationships between 2 Entities, especially if one Entity can't act for itself.

An authority can be:

Role-based: parents/guardians of children, directors of companies, attorney of a client

- Roles and powers are often legislated and context-specific

Delegated: employees in a team, siblings in a family, spouse or partner in a relationship

- A delegating Entity can't grant any more power than they hold themselves

This guidance describes verifying if someone has an authority to act.

Different authorities require different approaches that are very dependent on the context for why an authority to act has been given.

Training, clinics and resources

Online training

Free e-learning modules available at the Leadership Development Centre: https://www.ldc.govt.nz/

Identification Essentials

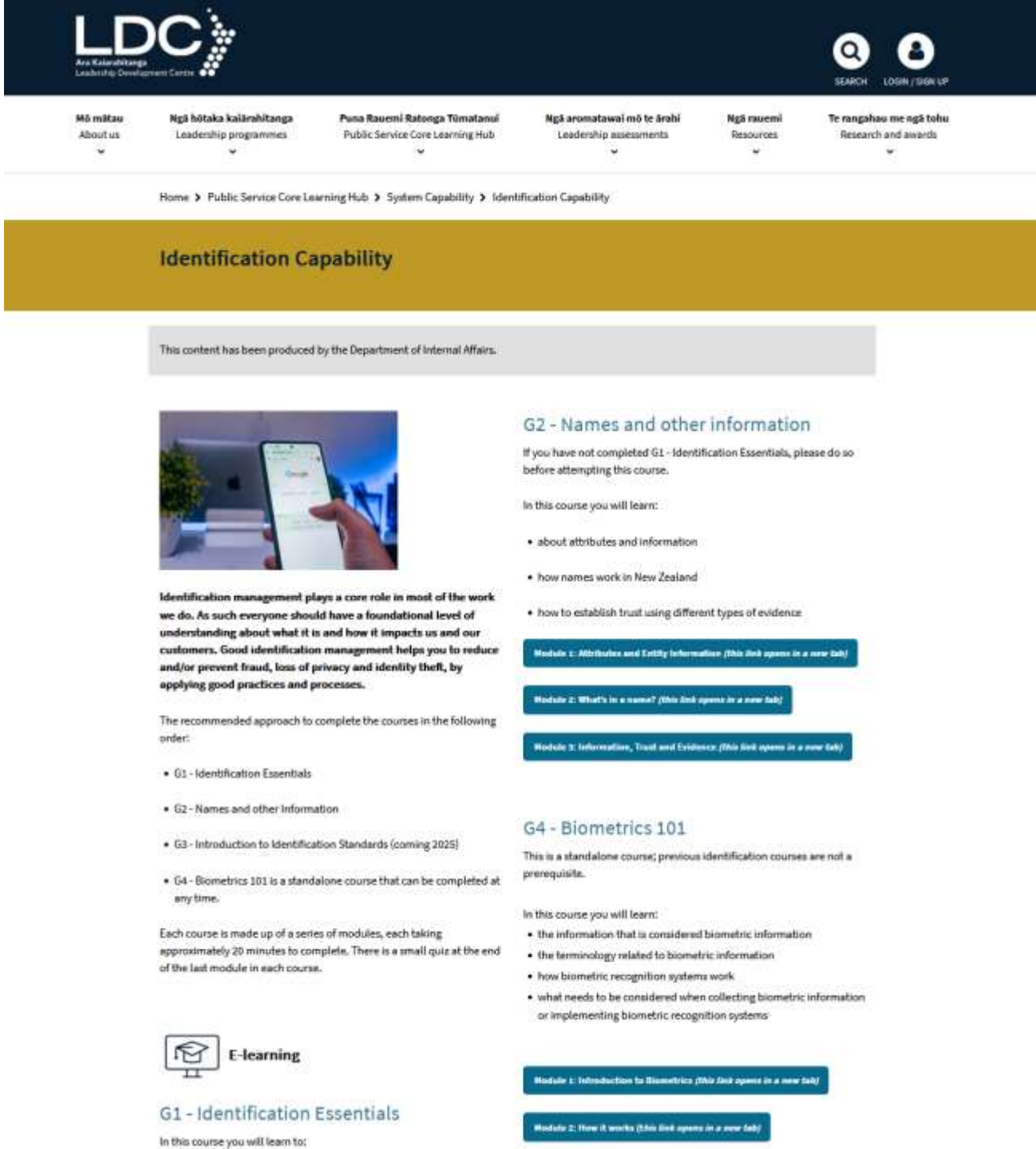
Understand key terms, recognise processes, and apply processes to reduce identity theft.

Names and other information

Learn about attributes, how names work in New Zealand, and how to establish trust.

Biometrics 101

Information and terminology, how biometric systems work, and what you need to consider.



Clinics

Drop-in sessions held on the first Wednesday of every second month, 2pm to 4pm.

Upcoming clinic sessions for 2026:

- **3 June** — Why photocopies are bad
- **5 August** — Levels of Assurance
- **7 October** — Identifiers revisited: National, centralised and decentralised
- **2 December** — Why Binding and Authenticators are key

Enrol by emailing IdMStandards@gdda.govt.nz

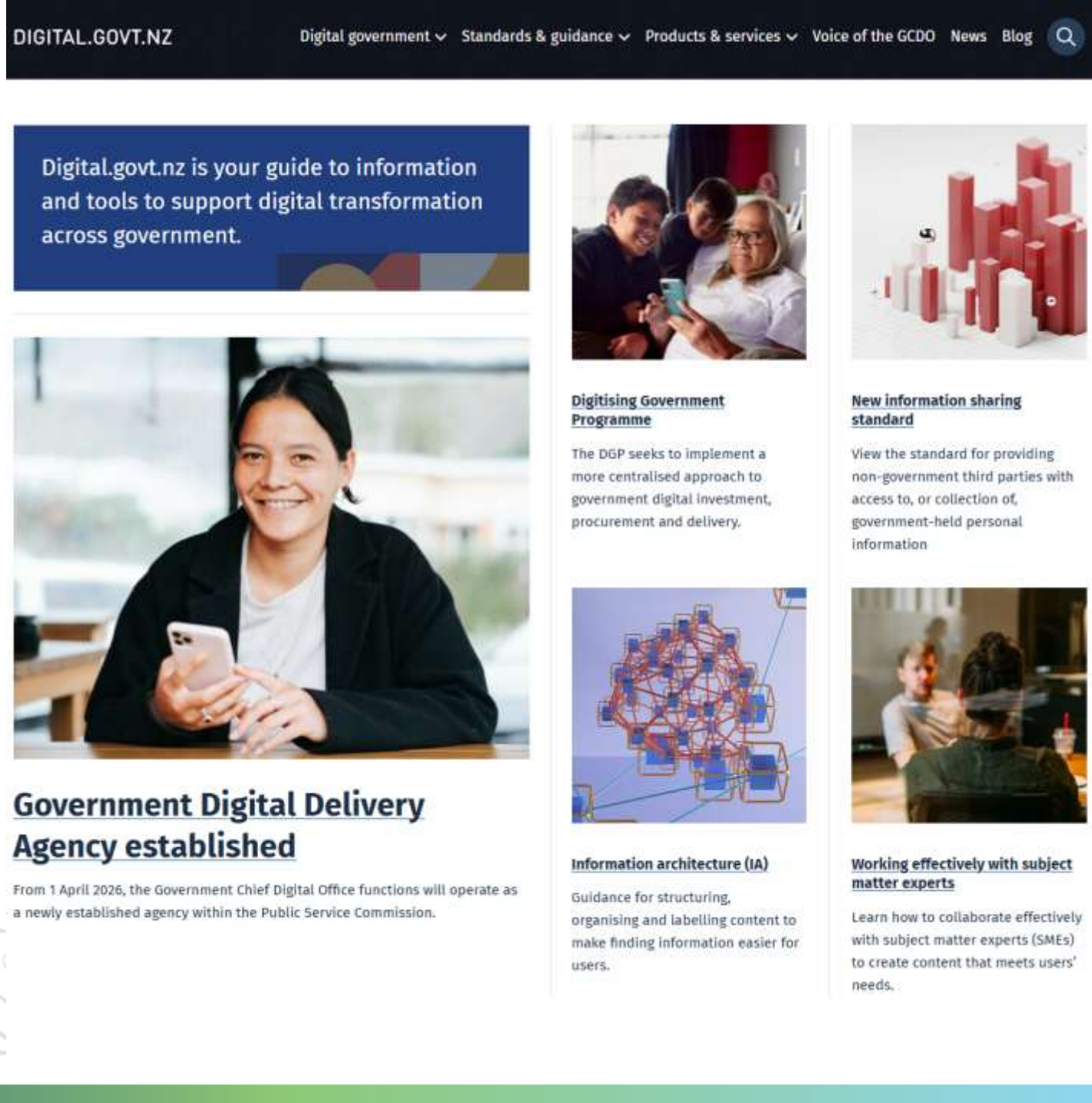
Digital.govt.nz

Resources, guidance, the Standards, and more:

https://www.digital.govt.nz/

Contact us and sign up for online training!

IdMStandards@gdda.govt.nz



Summary

- Identification supports good privacy and security practices.
- Good identification is managing risk. Managing identification risk overlaps with managing privacy and security risks.
- When you measure your risk you know what level of assurance you need.
- Like privacy and security, identification is a core skill.
    - We offer free courses on how to do Identification Management.
- We’re here to help with training, guidance, and advice.
- We need to embed identification in our systems and organisations to turn the tide on identity theft, and the fraud that stems from it!

Pātai / questions

Government Digital Delivery Agency
Te Pūnaha Matihiko

Tēna rawa atu koutou
Thank you very much

Icons in this presentation are attributed to flaticon.com