Security as a Service – A Low Risk Approach to Integrating with NEHTA’s Security Specifications

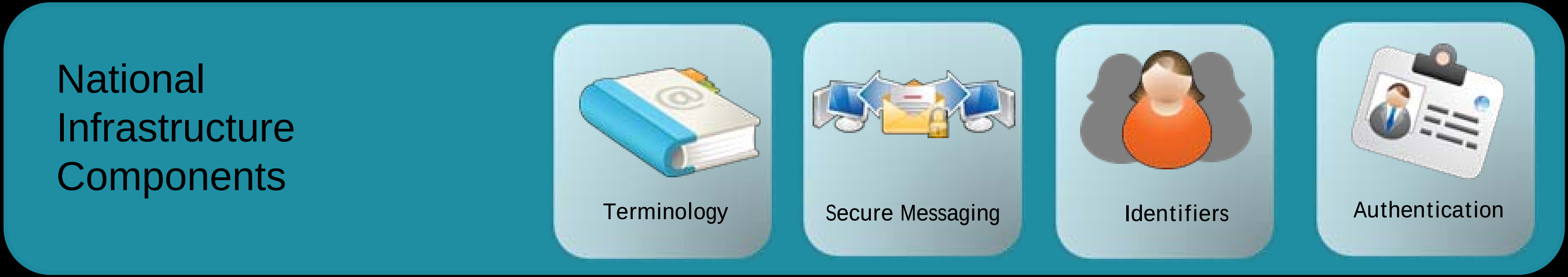
Neil Readshaw

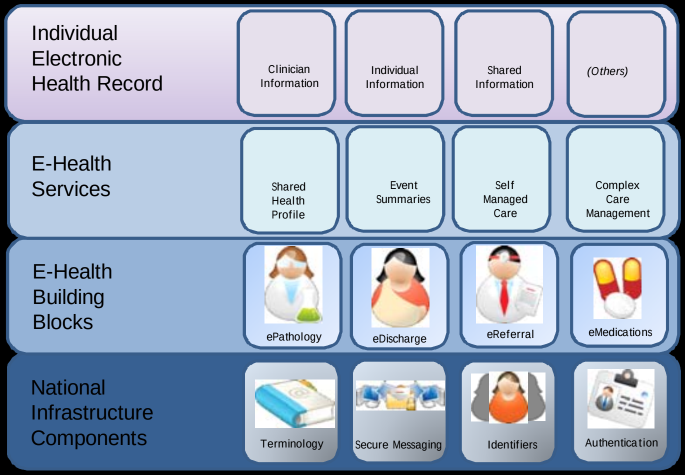
IBM Australia Development Laboratory

Introduction

- Successful e-Health transition requires a strong security and privacy foundation
- NeHTA is stewarding a set of specifications to provide this foundation
- Migrating all IT systems to become NeHTA-aware could be complex, time-consuming and risky for some organisations
- This presentation offers an approach that is focused on maximising reuse of existing IT assets

National Infrastructure Components defined by NeHTA



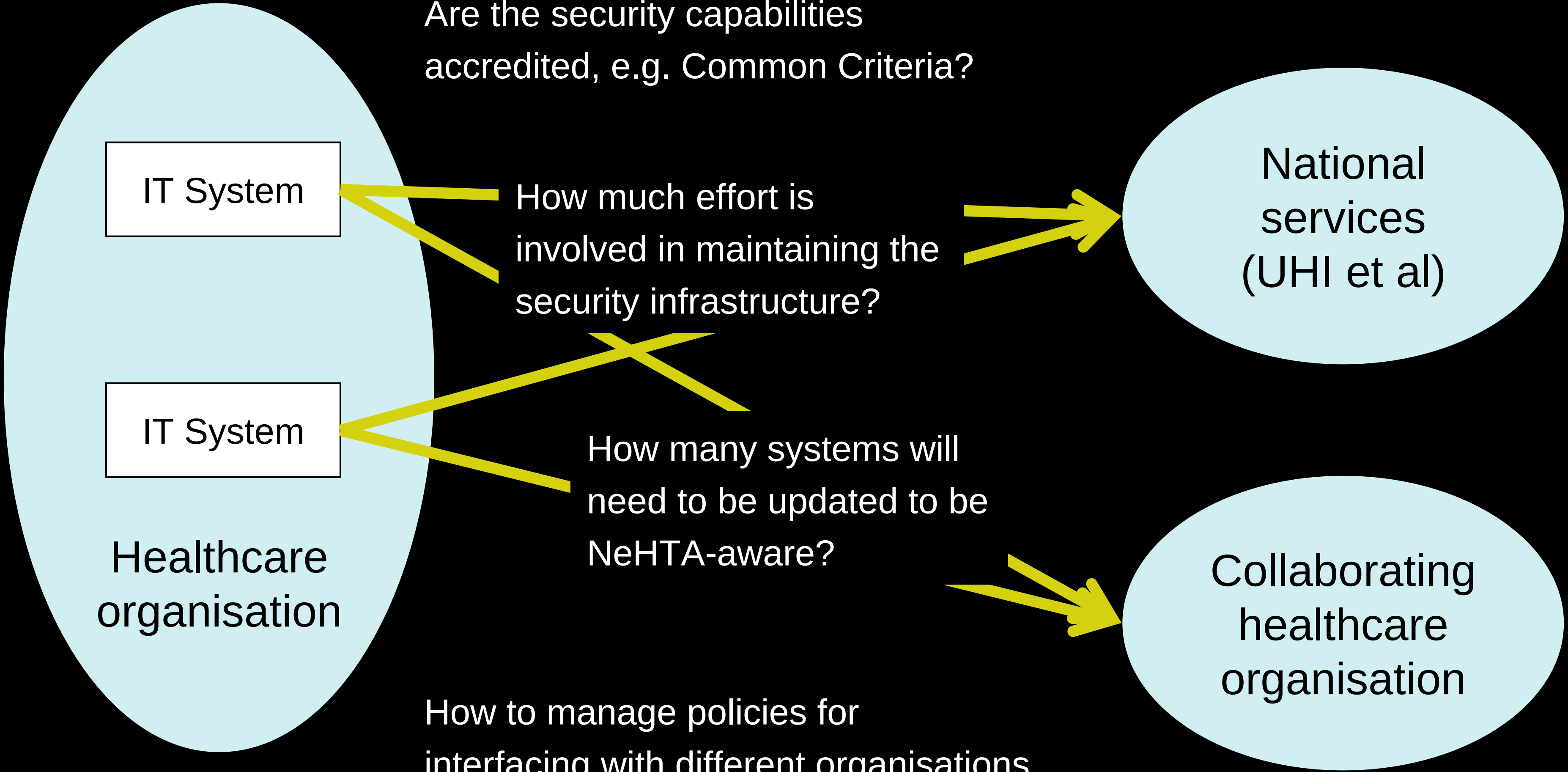


e-Health Services Stack

Infrastructure Component	Benefit
Secure Messaging	Confidentiality of personal healthcare information
UHI (Unique Healthcare Identifier)	Correlation of identity information across disparate systems and organisations
NASH (National Authentication Service for Health)	Strong authentication credentials

Source: NeHTA

Security considerations when integrating with the National Infrastructure Components


IT System
IT System
Healthcare organisation
National services (UHI et al)
Collaborating healthcare organisation

Are the security capabilities accredited, e.g. Common Criteria?

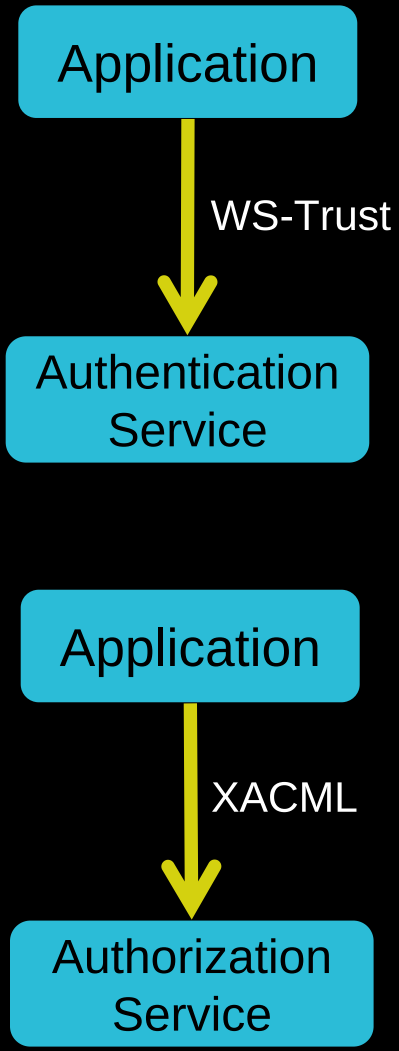
How much effort is involved in maintaining the security infrastructure?

How many systems will need to be updated to be NeHTA-aware?

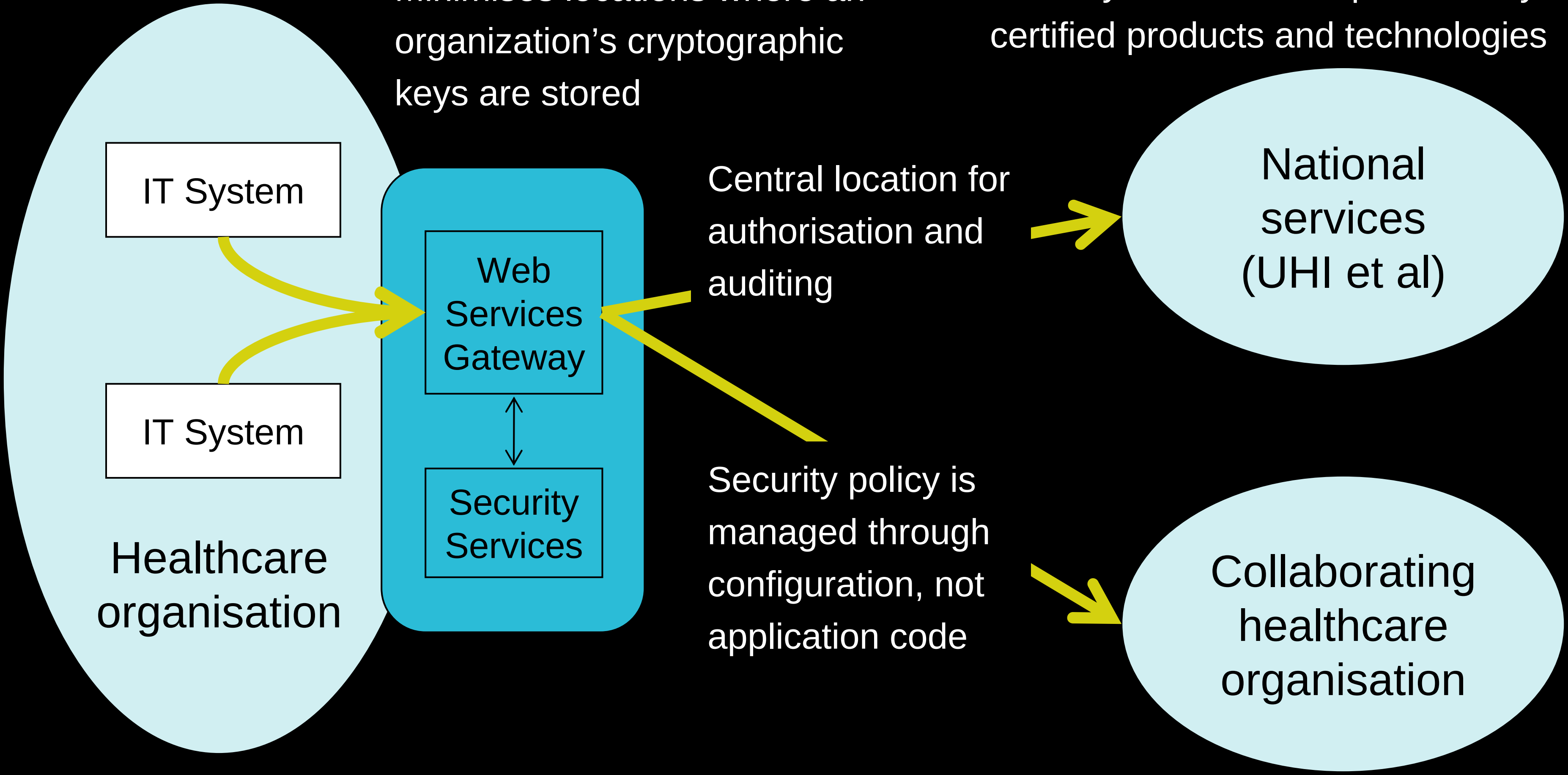
How to manage policies for interfacing with different organisations using different security profiles?

An Alternate Approach using Security Services

- Security Services have characteristics based on Service Oriented Architecture principles
  - Repeatable
    - Each service provides a repeatable security function, e.g. authentication, authorization
  - Reusable
    - Security services can be integrated with multiple systems
  - Agile
    - Changes in security technologies/policies are externalised from applications, and become configuration, not coding tasks
  - Built using open standards
    - Simplifies interoperability



... A Secure Approach



Minimises locations where an organization’s cryptographic keys are stored

Security infrastructure provided by certified products and technologies

IT System

IT System

Healthcare organisation

Web Services Gateway

Security Services

Central location for authorisation and auditing

National services (UHI et al)

Security policy is managed through configuration, not application code

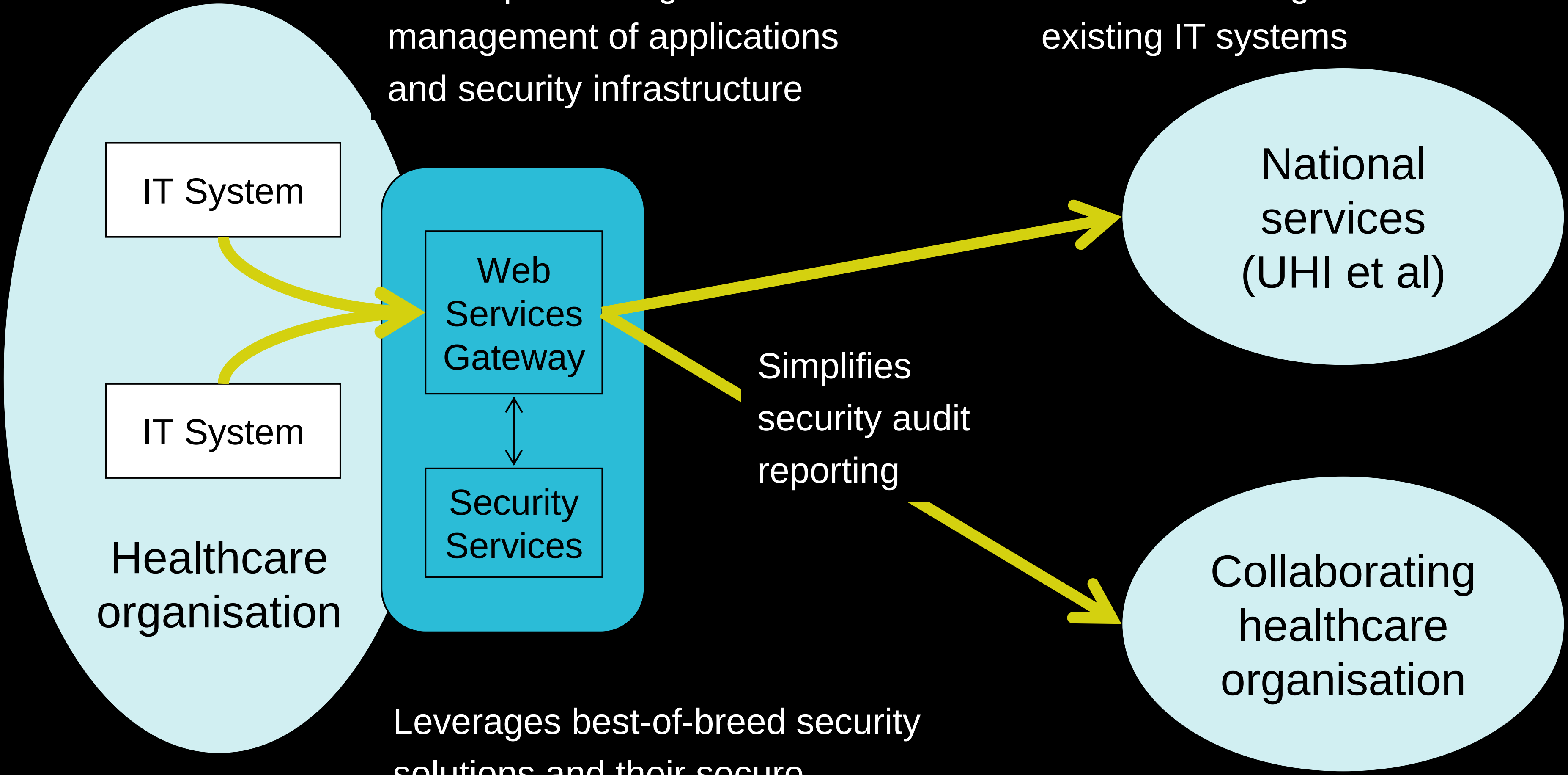
Collaborating healthcare organisation

eHR information may be filtered based on organisational or government privacy constraints

... A Low Risk Approach

De-couples change management of applications and security infrastructure

Minimises changes to existing IT systems

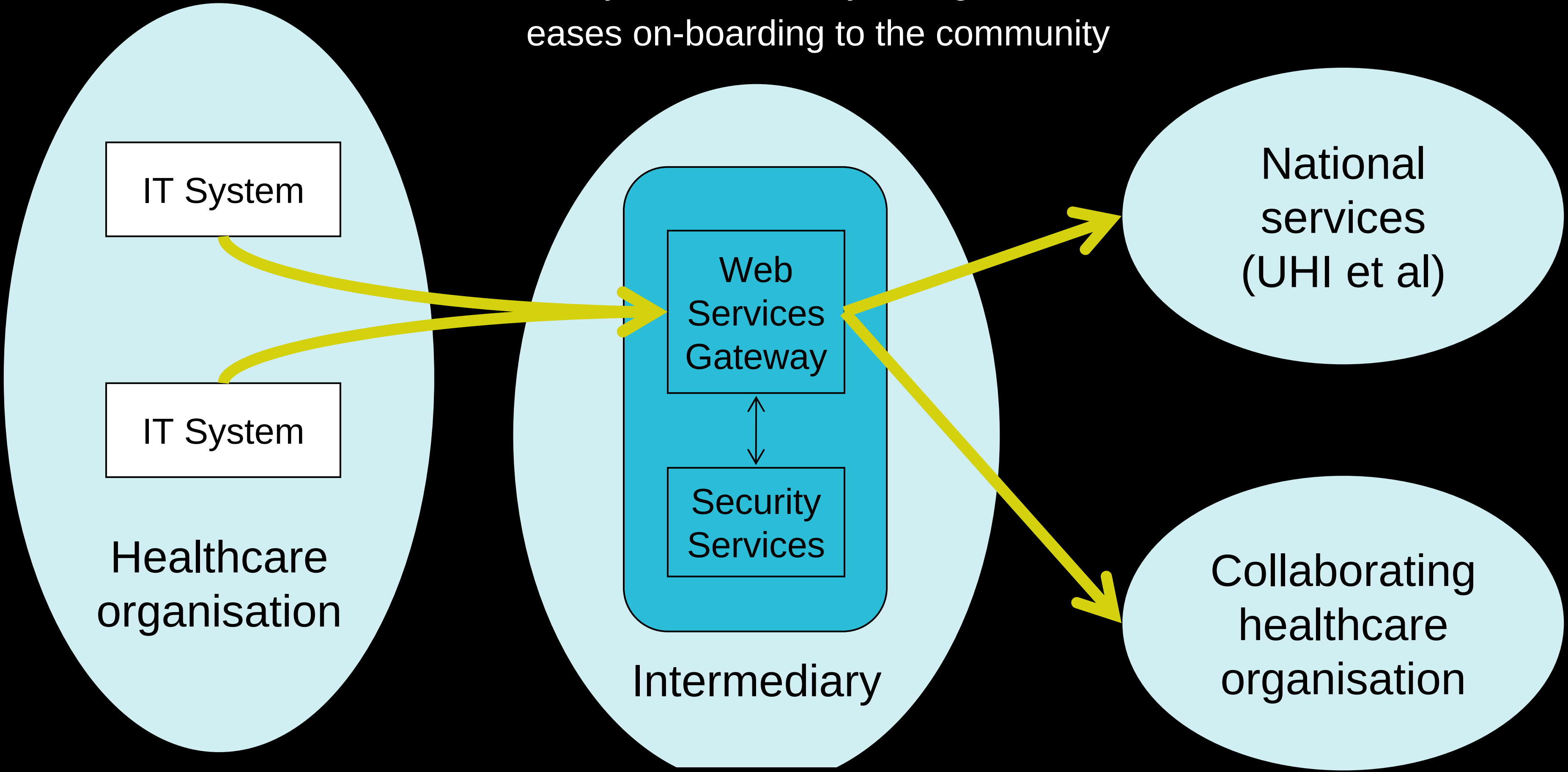


Simplifies security audit reporting

Leverages best-of-breed security solutions and their secure development methodologies

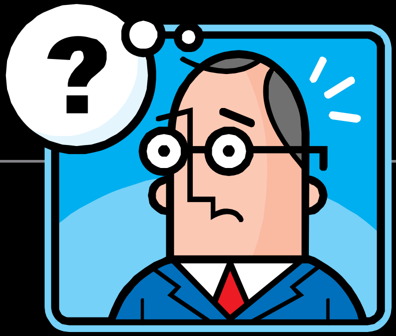
... Suitable for Intermediaries too

Policy driven security configuration eases on-boarding to the community



Intermediary becomes the NeHTA interface for the entire community

But what about...



- Does this mean that all applications have to be converted to SOA?
  - No, but the applications will need to communicate with the Web Services Gateway *somehow*, including asserting the user identity.
- Would all applications have to use the same authentication scheme, such as PKI?
  - Not necessarily. Users may continue to authenticate as they do today. Their identity is converted to a NeHTA compliant form by the authentication service integrated with the Web Services Gateway
- How practical is the Security as a Service vision?
  - Products are available today from multiple vendors
  - IBM example: WebSphere DataPower XML Firewall, Tivoli Federated Identity Manager, Tivoli Security Policy Manager

Practical Considerations

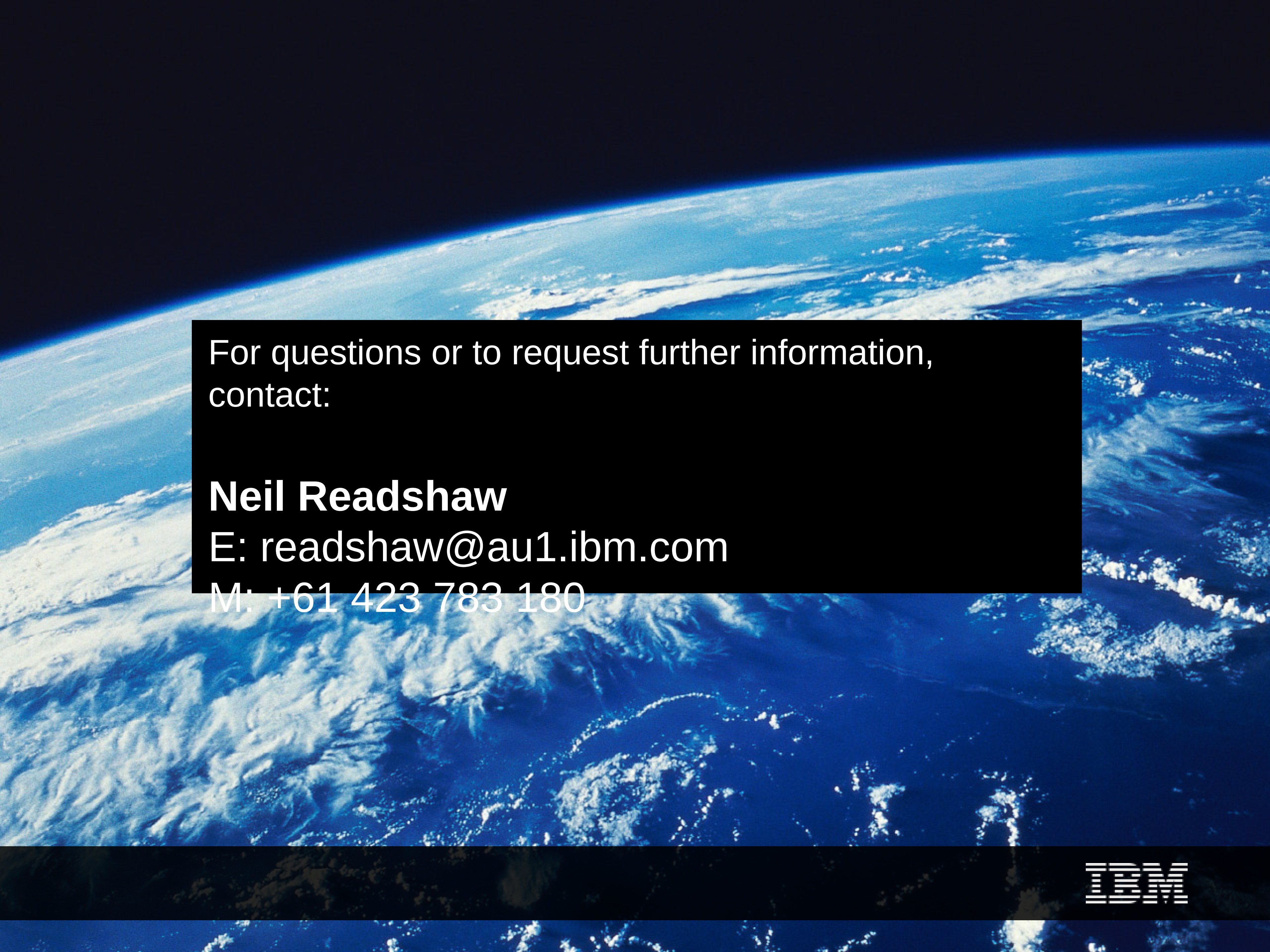
- The devil is in the security integration detail
  - Use tools that offer flexibility so interoperability issues can be identified and resolved
  - Leverage opportunities for interoperability testing

- Plan for change while interoperability profiles stabilise
  - Look for solutions where security policies can be re-configured with no change to application code

- Use devices capable of wire speed XML processing to mitigate performance considerations when using message level protection
  - Example: XML accelerators/appliances

Summary: the Security as a Service approach:

- Reduces the number of IT systems that need to implement NeHTA specifications
- Provides central management of security policies (authentication, authorization, message protection, ...)
- Is policy driven, so that incorporating new security technologies means a change in configuration, not re-development
- Uses products and technologies with security accreditation



For questions or to request further information, contact:

Neil Readshaw
E: readshaw@au1.ibm.com
M: +61 423 783 180