Validation of ebXML Messaging for use with eGovernment

OASIS e-Government TC

Graham Beaver
Senior Solutions Architect
HP EMEA Government Practice

Agenda

- Introduction
- Concepts
- Issues
- Possible Solutions
- Conclusions
- Work To be Done

Introduction

Use of ebXML in e-Government

- European Union – Interchange of Data between Administrations (IDA)
  - Trans-European Telematics Networks for Administrations
- NATO
  - C3 Technical Architecture
- UK Government
  - eGIF
- US Government
  - Federal Enterprise Architecture – Technical Reference Model
- .....

Objective

"Give an overview of the use of the ebXML Message Service with Government, and initial thoughts on the issues and possible solutions to these issues."

Concepts

Scope

- Citizen to Government
  - C2G / G2B
- Business to Government
  - B2G / G2B
- Intra-Departmental
  - E2G / G2E
- Interdepartmental
  - D2D
- Inter-Governmental
  - G2G

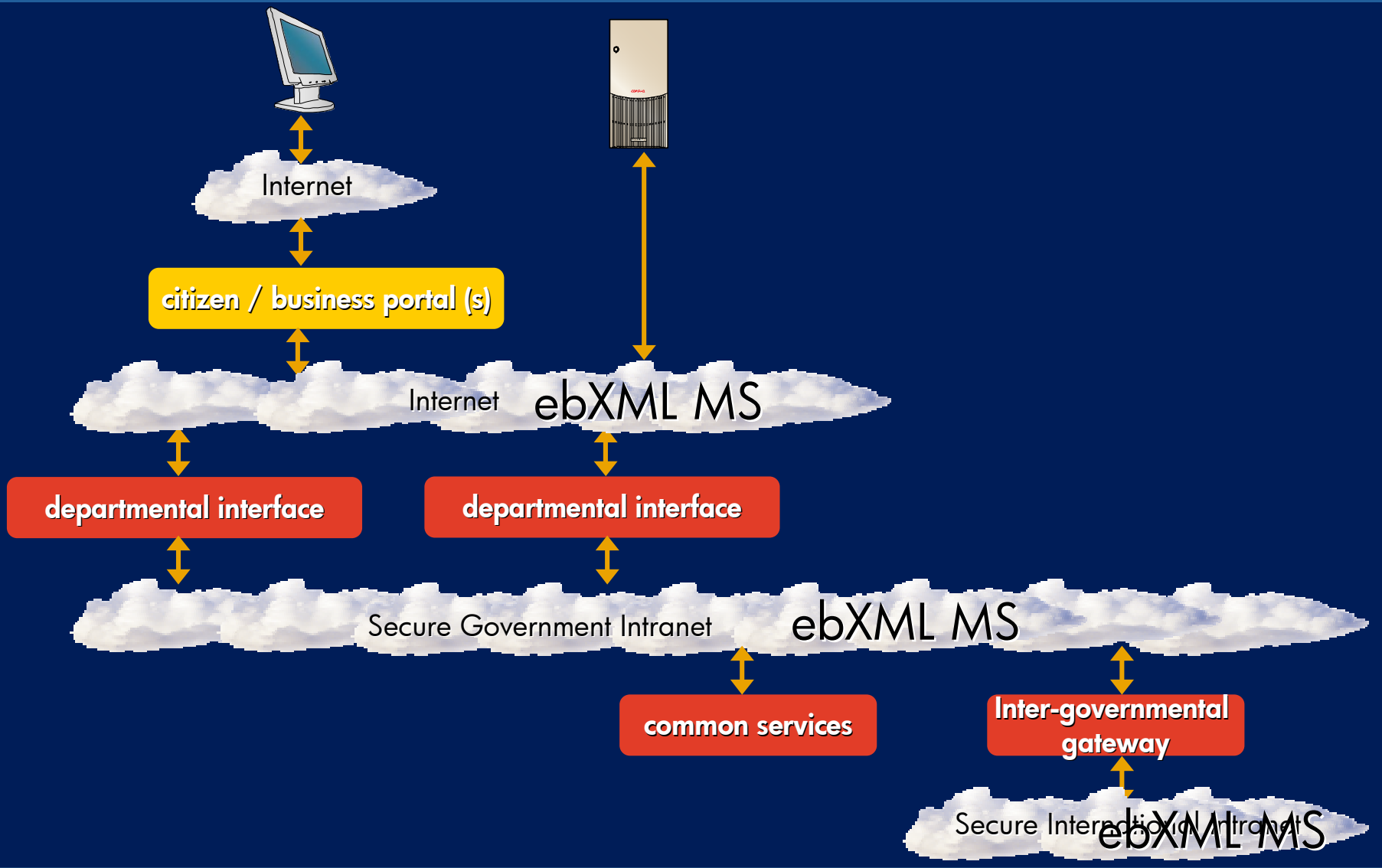
Service Delivery Models

- Department Centric Service Delivery
- Government Centric Service Delivery
- Citizen Centric Service Delivery

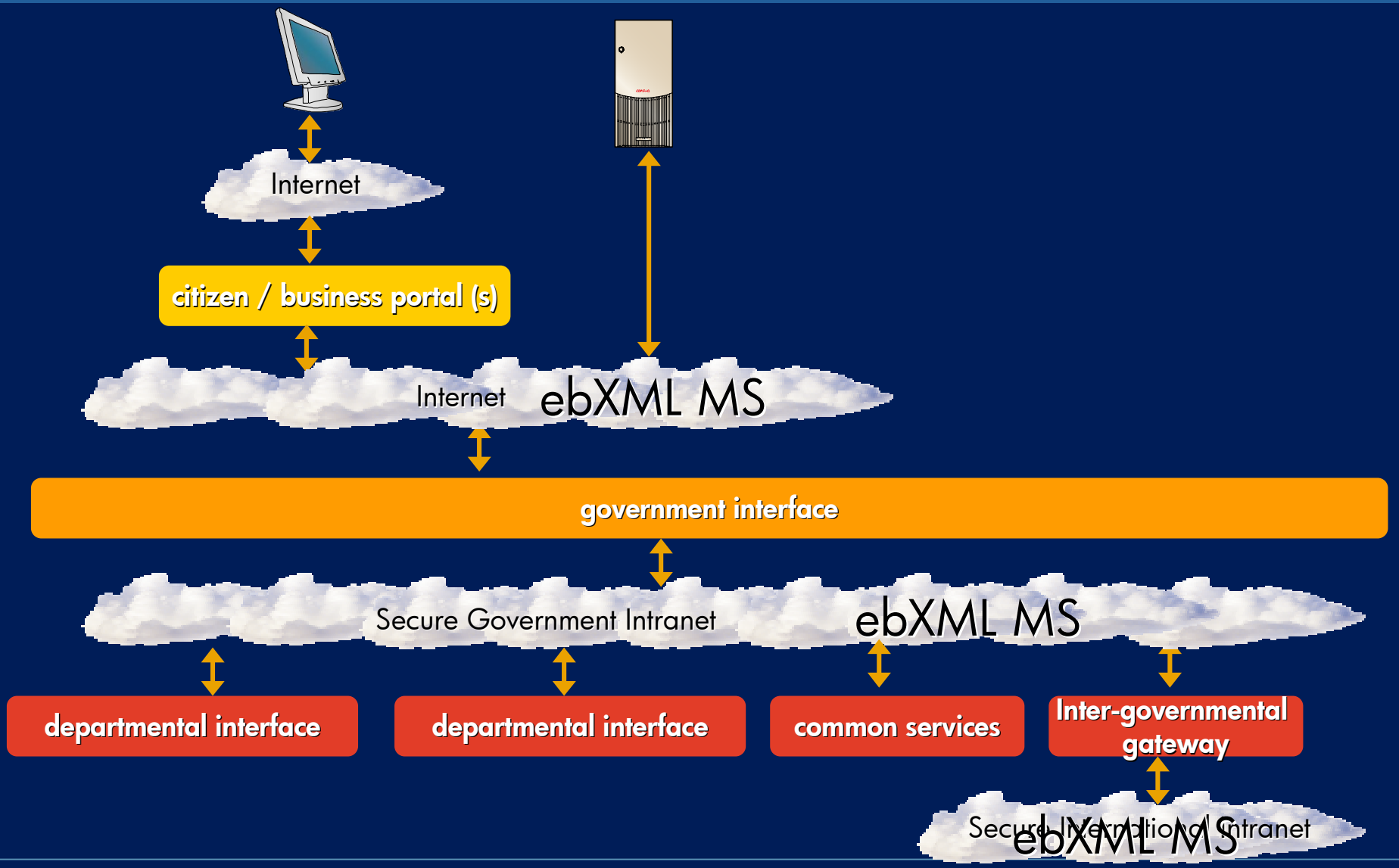
Government Infrastructure Components

- Portal
- Call Centre / Face-2-Face
- Governmental Interface
- Departmental Interface
- Common Services
- Inter-Governmental Interface

Common Architectures



Common Architectures



Originating Actors

- Principle Subject
  - identified by unique Ids used the the Government Department whose service is being used.
    - such as
      - health number,
      - passport number,
      - social security number,
      - …. or combinations
      - Government Department ID

Originating Actors

- Requesting Subject
  - citizen / public sector employee requesting service on for the principle subject ids
    - such as
      - instance of the principle subject
      - parent / guardian of a child
      - professional (such as accountant)
      - public sector employee (i.e . purchasing staff)

Originating Actors

- Actioning Subject
  - Citizen / public sector employee / line of business application who actually interacts with the system / transaction
    - such as
      - the instance of the principle subject
      - the instance of the requesting subject
      - public sector employee (e.g. call centre staff, face-2-face)
      - line of business application (e.g. payroll / accounting application)

Originating Actors

- Examples
  - one subject (citizen on portal)
    - service
      - tax return via a portal
    - principle subject
      - Name = Person A
      - Tax Reference = 123456789
    - requesting and actioning subject
      - Person A (identified by digital certificate)

Originating Actors

- Examples
  - different principle and requesting subject (parent of child on portal)
    - service
      - make medical appointment
    - principle subject (child)
      - name = Person A
      - health number = 234567A
      - date of birth = 2003-05-01
    - requesting and actioning subject (parent / guardian)
      - Person B (identified by Digital Certificate)

Originating Actors

- Examples
  - different principle and requesting subject (public sector employee on portal)
    - service
      - financial return to statistics office
    - principle subject
      - department = Ministry of Defence
    - requesting and actioning subject
      - Person A (identified by digital certificate)

Originating Actors

- Examples
  - different principle, requesting and actioning subject (parent of child to call centre)
    - service
      - make medical appointment
    - principle subject (child)
      - name = Person A
      - health number = 234567A
      - date of birth = 2003-05-01
    - requesting subject (parent / guardian)
      - Person B (identified by Digital Certificate)
    - actioning subject (call centre staff)
      - Person C (identified by Digital Certificate)

Issues

Issues

- Introduction
  - analysis of different types of transactions using ebXML message envelopes using different architectures

Issues

- Authentication of each subject
  - requesting subject
  - actioning subject
  - the authentication credentials of each subject may need to be contained within the ebXML message envelope for validation at multiple stages during the transaction.
    - (discuss ??)

Issues

- Authorisation of each subject to act upon the behalf of the other subject for a service
  - ensuring that the:
    - the requesting subject is authorised to access the service using the principle subject ids
    - the actioning subject is authorised to access the service on behalf of the requesting subject
  - ensuring the authorisation credential is included into the ebXML message envelope for validation at multiple stages of the transaction

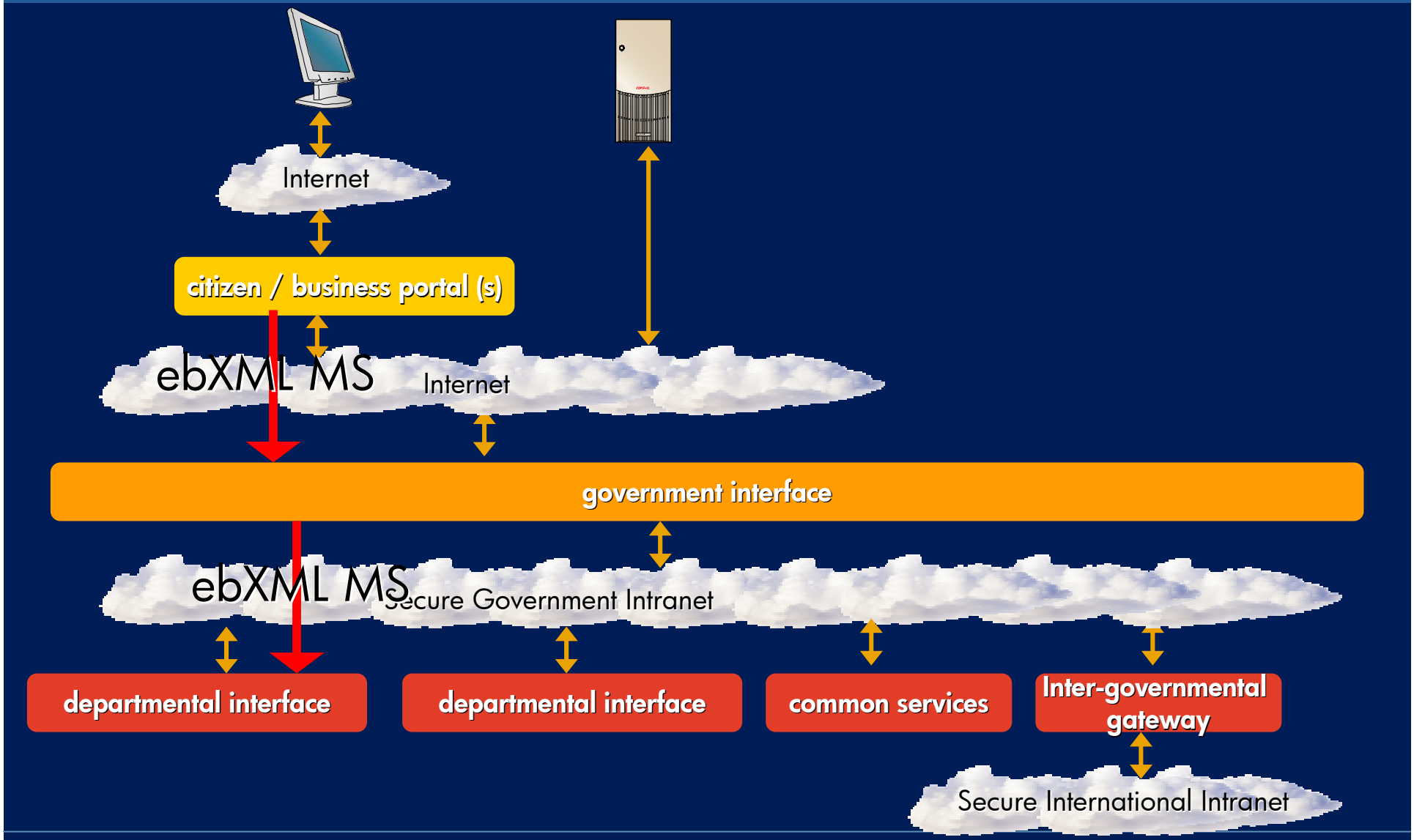
Issues

- Allow for different authentication levels by service
  - each service may require different level of authentication credential
    - such as:
      - password / pin
      - soft digital certificate
      - hard digital certificate (smart card)
      - bio-metric
    - the credential type must be of each subject may need to be contained within the ebXML message for validation at multiple stages during the transaction

Issues

- Unknown end point of communication
  - Government Centric Service Delivery
    - the ebXML MS ‘To’ element can not correctly completed by the Portal nor Line of Business Application.
    - multiple different ebXML messages, with different creators
      - portal
      - government interface
    - same transaction !!

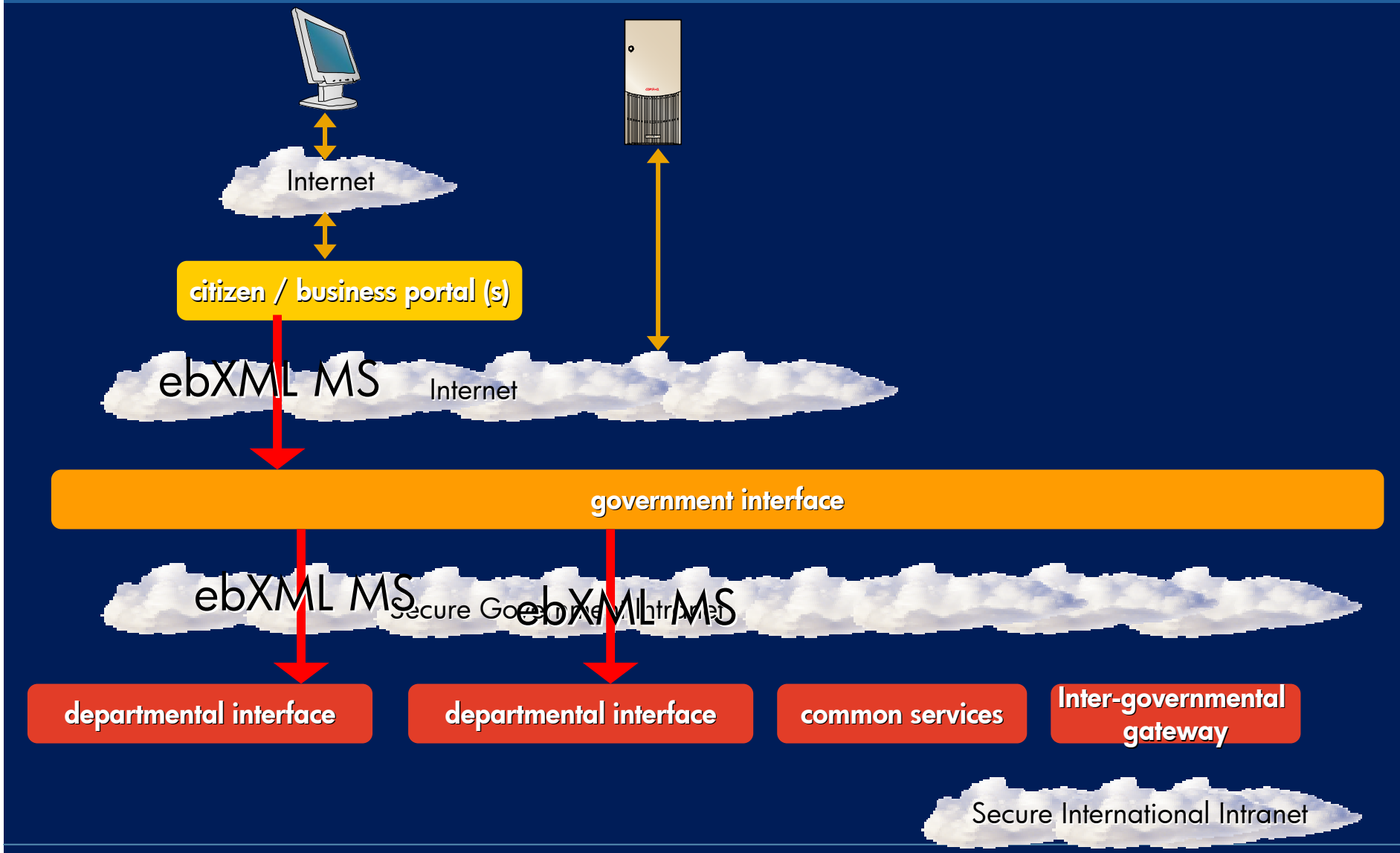
Unknown end point of communication



Issues

- Multiple end-points for communication
  - Government Centric Service Delivery
    - the ebXML MS 'To' element can not correctly completed by the Portal nor Line of Business Application.
    - multiple different ebXML messages, with different creators
      - portal
      - government interface
    - same transaction !!

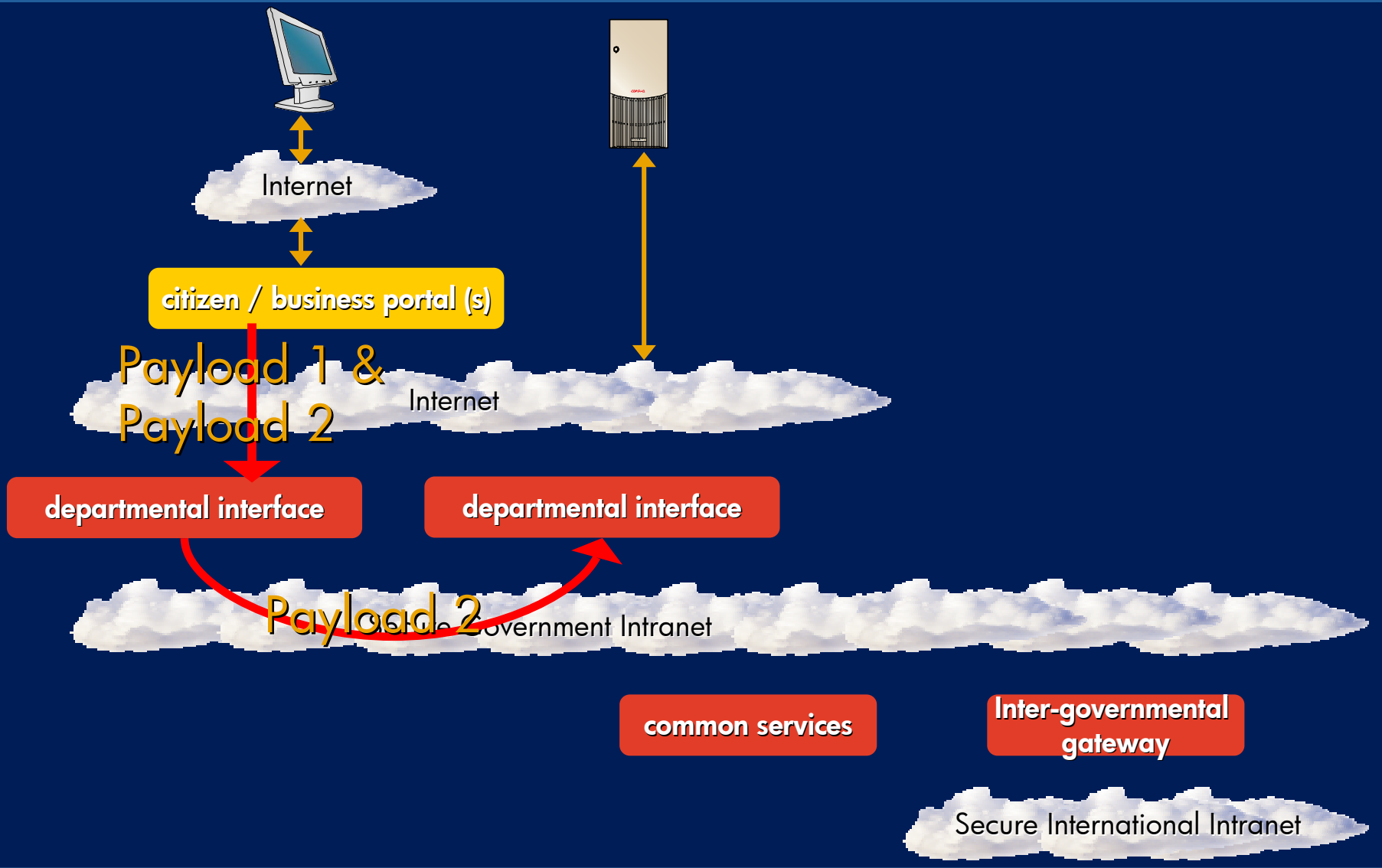
Unknown end point of communication



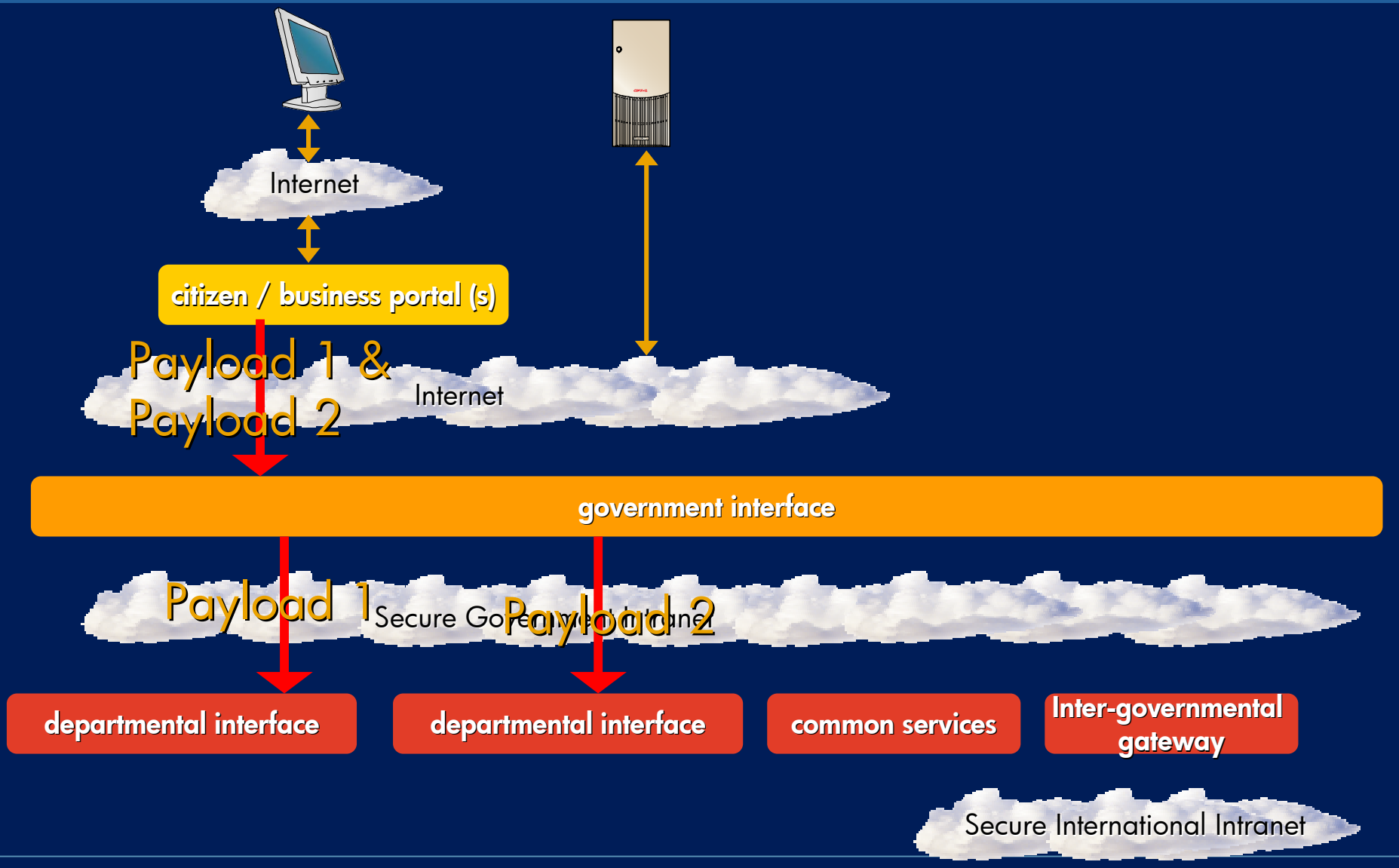
Issues

- Allowing for message splitting
  - Governmental Centric Service Delivery
  - Departmental Centric Service Delivery
    - ensuring that integrity of the payloads is maintained
  - Same transaction !!

Message Splitting



Message Splitting



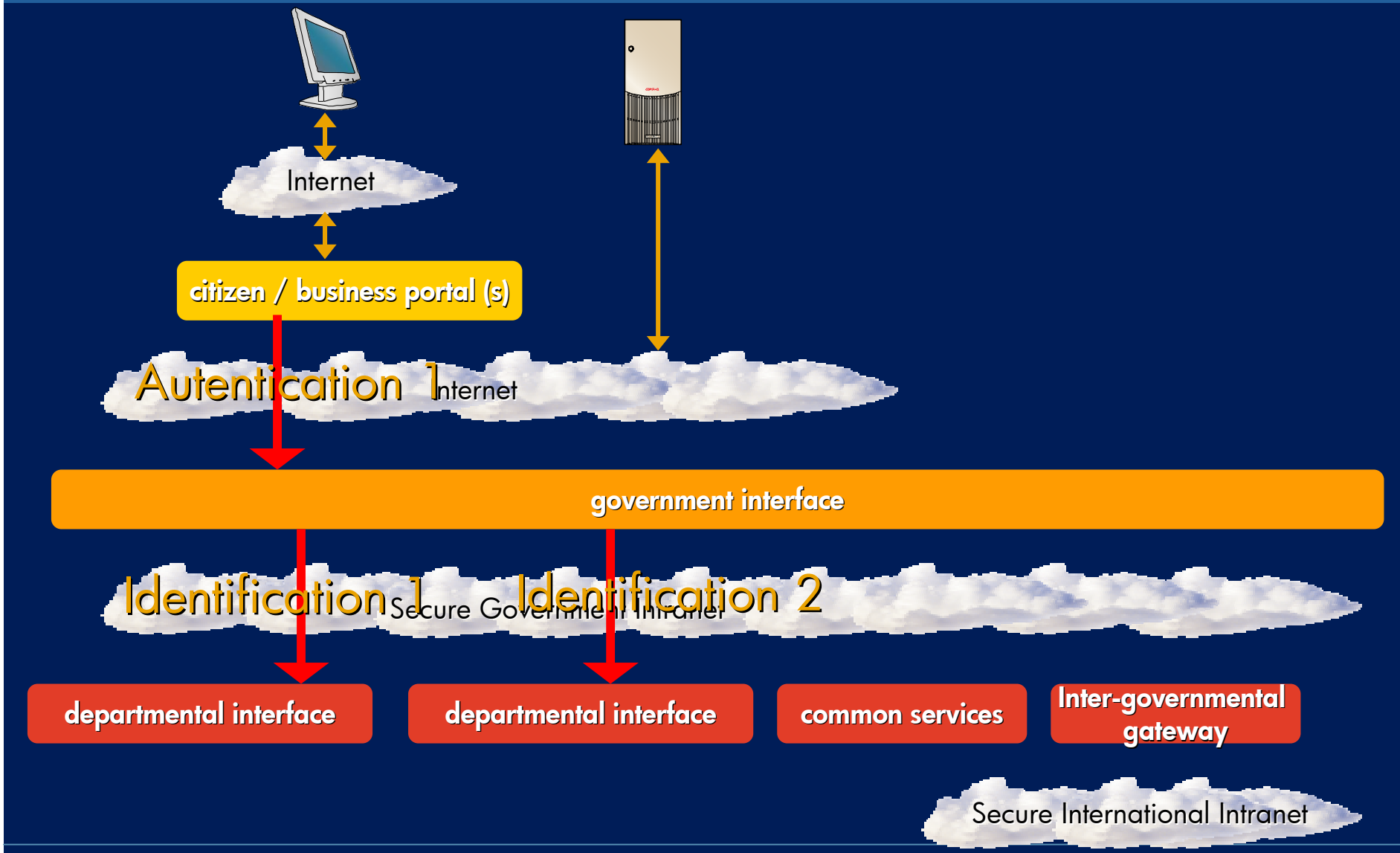
Issues

- Ensure the integrity of each payload item
  - allowing for payloads to move from envelop to envelop.
  - allowing multiple payloads from one envelope to be separated into multiple different envelopes whilst maintaining (and proving) the integrity of each payload

Issues

- Ensuring only relevant identification credentials are distributed

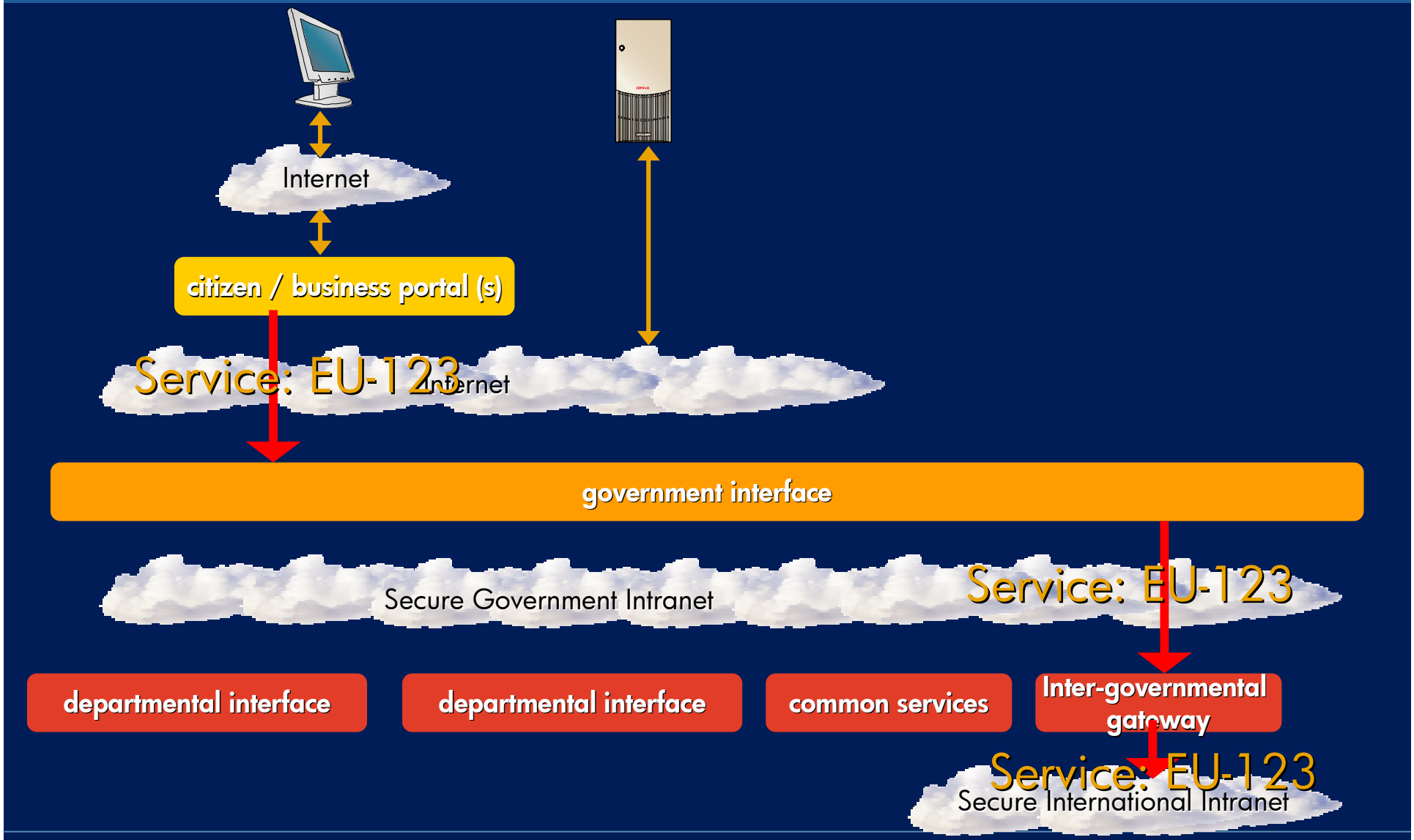
Only relevant credentials are distributed



Issues

- Ensure the Global uniqueness of all identifiers across the whole of Global Government
  - Governmental Centric Service Delivery
    - service delivery may span more than one level of government within a country
    - service delivery may span more than one country

Global uniqueness of identifiers



Issues

- Ensure the integrity of the Timestamps
  - allow for the legal status of the ebXML messaging entering Government
    - allow for the timestamp to be forwarded with all sub messages
      - (discuss ??)

Possible Solutions

Solution Concepts

- Use of existing Standards
  - OASIS
  - W3C
  - IETF
  - ……

Solution Concepts

- W3C
  - XML Signature Syntax and Processing
- OASIS
  - SAML

Global Uniqueness

- ebXML Message Service Specification
  - From element (and To element)
    - base ebXML Specification

```
<eb:From>
        <eb:PartyId eb:type="urn:duns">123456</eb:PartyId>
        <eb:Role>http://rosettanet.org/roles/buyer</eb:Role>
</eb:From>
```

    - Government ebXML Specification

```
<eb:From>
        <eb:PartyId eb:type="urn:egXML:PartyId">UK-123456</eb:PartyID>
        <eb:Role>http://oasis-open.org/egXML/roles/….</eb:Role>
</eb:From>
```

Global Uniqueness

- ebXML Message Service Specification
  - ConversationId Element
    - base ebXML specification

      <eb:ConversationId>20030506-13345-3567</eb:ConversationId>

      – Only needs to be unique within the context of the CPAId
    - Government ebXML Specification

      <eb:ConversationId>UK-1234-20030506-1</eb:ConversationId>

      – Pattern:

        – CountryCode-NodeId-Date-ConversationID

      – Globally Unique

Global Uniqueness

- ebXML Message Service Specification
  - Service Element
    - Base ebXML Specification

      <eb:Service>urn:services:SupplierOrderProcessing</eb:Service>

      must only be unique between trading partners
    - Government ebXML Specification

      <eb:Service >urn:services:UK-BenefitApplication-2003-01</eb:service>

      – Pattern

      – CountryCode-ServiceName-Year-Version

      – Globally Unique

Global Uniqueness

- ebXML Message Service Specification
  - MessageId Element (and RefToMeassage)
    - Base ebXML specification

      <eb:MessageId>20030506-133003-14@example.com</eb:MessageId>

      Globally unique if compliance with RFC2822 is achieved
    - Government ebXML specification

      <eb:MessageID>UK-12-20030506-01-01@egXML.org</eb:MessageId>

      – Pattern

        – CountryCode-NodeId-Date-MessageNumber-PartNumber

      – Globally Unique

      – Additional Data

        Allows for larger messages to be split and maintained in order

Authentication and Authorisation

- SAML
  - Inclusion of SAML Assertion within ebXML Header
  - SAML Assertion produced by Trusted Government Authentication and Authorisation Service
    - AuthenticationStatement
      - For Actioning and Requesting Subjects
    - AuthorisationStatement
      - For Actioning and Requesting Subjects for the Service
    - AttributeStatement
      - For Principle Subjects Identifiers
        - May be different AttributeStatements per Envelope if Message Splitting.

Authentication and Authorisation

- SAML
  - Digital Signature of SAML Assertion as per Specification to allow for proof of integrity of Assertion.

Message Integrity

- Digital Signatures
  - Payloads
    - By Payload Originators (citizen, business, Government)
      - Each Payload Signed Individually and Signature placed in egXML Payload Signature Block
        - Allows each payload to have a different end-point whilst still allowing for proof of message integrity.

Message Integrity

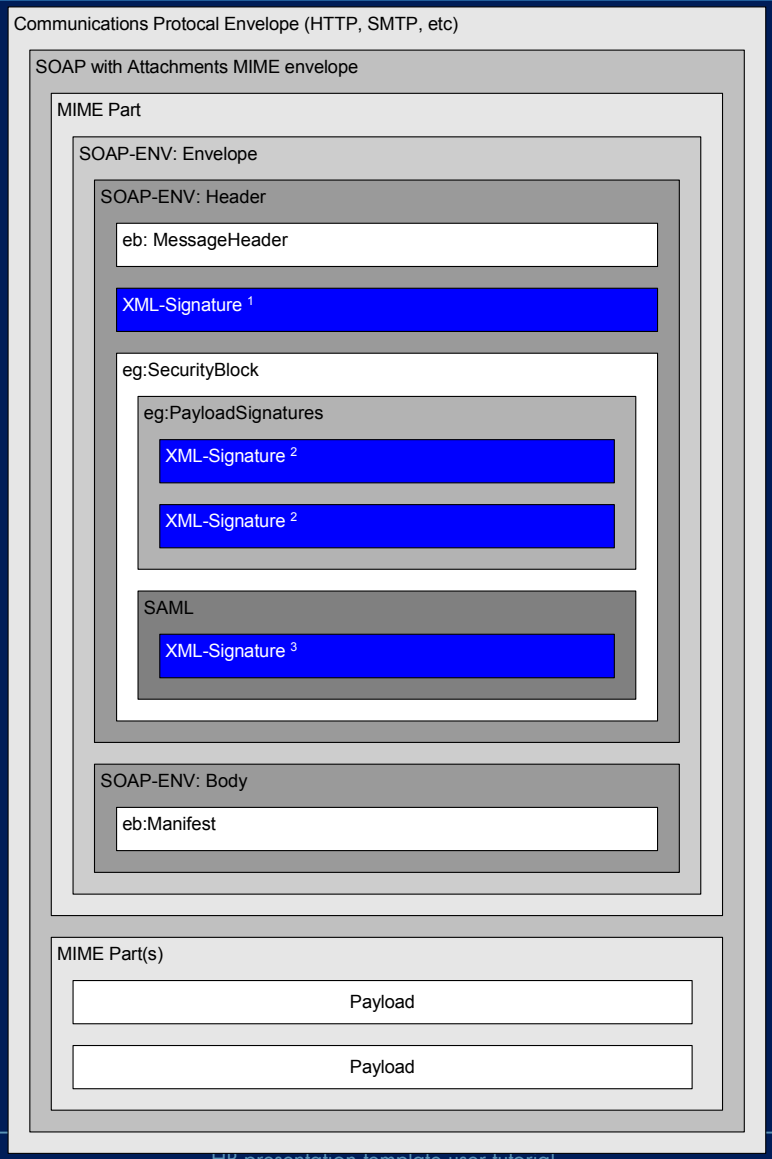
- Digital Signatures
  - ebXML Envelope
    - By Envelope Creator Message Service Handler
      - Signature to be placed with the ebXML Header as per ebXML specification.
      - Must include:
        - ebXML MessageHeader
        - Payload Signature Blocks
        - ebXML Manifest block
        - SAML Assertion

Global Uniqueness

- ebXML Message Service Specification
  - Payload ID
    - To ensure continued validation of the Payload Digital Signature the Payload reference must remain constant
      - To remain constant it must be globally unique.

        Content-ID: UK-123-20050506-1@egXML.org
      - Pattern
        - CountryCode-NodeID-Date-PayloadNumber

Government ebXML Specification



Usage

- ebXML Message Service Specification
  - Reliable Messaging Module
- ConversationId against MessageId
  - ConversationId flows from Envelope to Envelope with all the payloads

Conclusion

Conclusion

- With the additional elements and pattern refinements ebXML can be used for:
  - G2C / C2G
  - G2B / B2G
  - D2D
  - G2G

Work to be done

Work to be done

- Complete documentation
- Liase with OASIS ebXML Message Service TC
- Liase with OASIS SAML
- Get further Government buy-in
  - Wider Government Community
    - EU
    - NATO
    - Individual Governments

invent

BASIS