AS4 Communication Protocol profile

Workshop

Panagiotis Panousos

Business Area Manager, System Operation

Brussels – 09 Sep 2014

Role of ENTSOG

As laid down mainly in Article 4 of the Regulation, the role of ENTSOG is:

- to facilitate and enhance the cooperation between national gas of TSOs across Europe
- in order to promote the completion and functioning of the internal market in natural gas and cross-border trade
- and to ensure the optimal management, coordinated operation and sound technical evolution of the natural gas transmission network.

ENTSOG tasks under EU legislation

ENTSOG tasks are mainly defined within the Regulation (embedded in the 3rd Energy Package), as well as Regulation (EU) No 994/2010 ('Security of Supply') and Regulation (EU) No 347/2013 ('Energy Infrastructure Package').

Focusing on the Regulation, these tasks are mainly the following: the development of pan-European Network Codes ('**NCs**') for cross-border network and market integration issues, elaboration of an annual report, a pan-European Ten-Year Network Development Plan ('**TYNDP**'), the provision of regular gas supply and demand information for the European market and the delivery of common operational tools ('**CNOTs**') to ensure network security and reliability.

ENTSOG members

entsog

Introduction

- Results of Proof of Concept and updated AS4 Usage profile for TSOs published on ENTSOG website
- Material and notes / list of participants to be published

…we hope that this meeting will give you a better view on the future AS4 communication with TSOs …

Structure of event

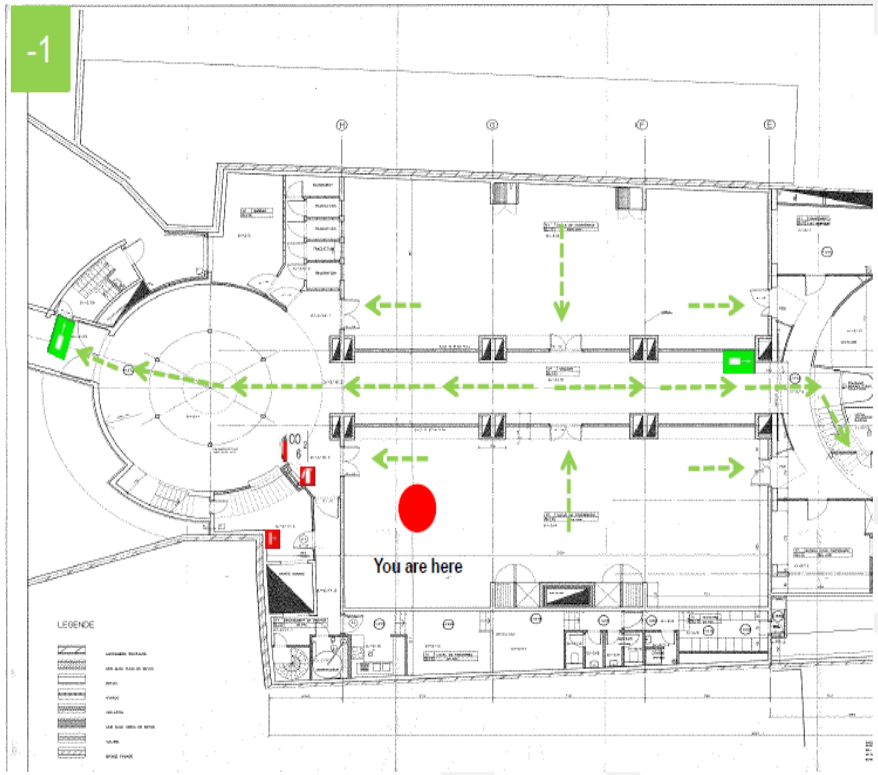
AGENDA

Please note all sections (other than the Welcome) will allow time for open discussion

No	Description	Time
1	**Opening** (ENTSOG: Panos Panousos) > Welcome / Introduction / Structure of Event > Objectives	**10:30-10:35**
2	**AS4 protocol profile** > Introduction / Requirements coming from INT NC (ENTSOG) > What is AS4 (ENTSOG) > The AS4 Usage Profile for TSOs (ENTSOG) > AS4 project example in Australia "SuperStream" (Axway) Discussion Panel (Q&A)	**10:35-11:45**
	Coffee Break	**11:45-12:00**
3	**AS4 proof of concept** > AS2 lessons learnt (EASEE-gas) > Proof of concept results and conclusions (ENTSOG) Discussion Panel (Q&A)	**12:00–12:45**
	Lunch	**12:45-13:45**
4	**AS4 proof of concept and next steps** > Participants' view: o **SNAM/Tibco** o **GCA/ADES** o **Westnetz/Seeburger** o **Gassco/Axway** > Further steps - implementation schedule, possible extensions (ENTSOG) Discussion Panel (Q&A)	**13:45-15:30**
	Coffee Break	**15:30-15:45**
5	**Conclusions and closing remarks**	**15:45-16:00**

- Objective: ENTSOG to present the outcome of Proof of Concept and explain AS4 Usage Profile
- How will this be achieved:
  - by presenting AS4 protocol and ENTSOG Usage Profile
  - by presenting views and intentions
  - by opening discussion panel and answering questions

Emergency Evacuation



- The evacuation plans are posted in each meeting room and indicated with signs.
- Emergency exits are to the street on Boulevard Charlemagne and on the rue Archimède.
- The assembly point is on Boulevard Charlemagne, in front of the Euroflat Hotel.

Thank You for Your Attention

Panagiotis Panousos
Business Area Manager, System Operation

ENTSOG -- European Network of Transmission System Operators for Gas
Avenue de Cortenbergh 100, B-1000 Brussels

EML: Panagiotis.panousos@entsog.eu
WWW: www.entsog.eu

AS4 communication standard

Jef De Keyser - ENTSOG
Pim van der Eijk – Sonnenglanz consulting

Brussels, 2014-09-09

Agenda

- **Introduction**
  - Data exchange and harmonisation
  - Network code Interoperability and Data Exchange – requirements and status
  - AS4 development

- **What is AS4**
  - Features of AS4 protocol

- **The AS4 Usage Profile for TSOs**
  - Details of AS4 Usage profile defined by ENTSOG

INTRODUCTION
-
Data exchange and harmonisation

Harmonisation - Why

Many parties involved in today's gas business

→ Need for harmonisation:

- **Cheaper** (less expertise and systems required for all communications) - # connections & partners
- **Simpler** (one system, one common protocol)
- **Faster** (set-up of new communication, only configuration, no coding required)

INTRODUCTION
-
Network code

Art 20 *General Provisions*

> Art 20: General provisions

- **What:** Regulation 715/2009 and accompanying regulations (CAM NC, BAL NC, CMP Guidelines, Transparency Guidelines)

- **Who:**
  - TSOs
  - TSOs – Network Users active at IP and VTP

Art 21 – *Common Data Exchange Solutions*

Components

- Data Network (= medium)
- Data Exchange Protocol (= language)
- Data Format (= vocabulary)

Types of Data Exchange - toolbox:

- **Document based (AS4 – Edig@s XML)**
  - Formatted files sent from one computer to another computer (electronic letter)

- **Integrated (web services – Edig@s XML)**
  - Direct data exchange between two computers

- **Interactive (web browser)**

For all DE types → network = Internet

Art 22 – Security and availability

> **Security:**

Each party shall:

- provide secure communications :
  - confidentiality
  - integrity and authenticity
  - non-repudiation
- implement security measures
- inform other parties in case of any problem

> **Availability:**

TSOs shall:

- avoid single points of failure
- obtain appropriate services
- minimize downtime
- inform their counterparties

Art 23 – Implementation

> **Common solution parallel to the existing solutions**

- **TSOs** shall make available and use the common data exchange solution defined under Art 21

- **Existing solutions** can stay if:
  - **compatible** with data exchange requirements
  - subject to **NRA approval** (after consultation with NUs)

→ Parties who cannot communicate with TSOs with their existing DE protocol shall also use the common DE solution

Art 24 – Development process for CNOT

- **For identified DE requirement under Art 20(2) ENTSOG shall develop common network operation tool.**

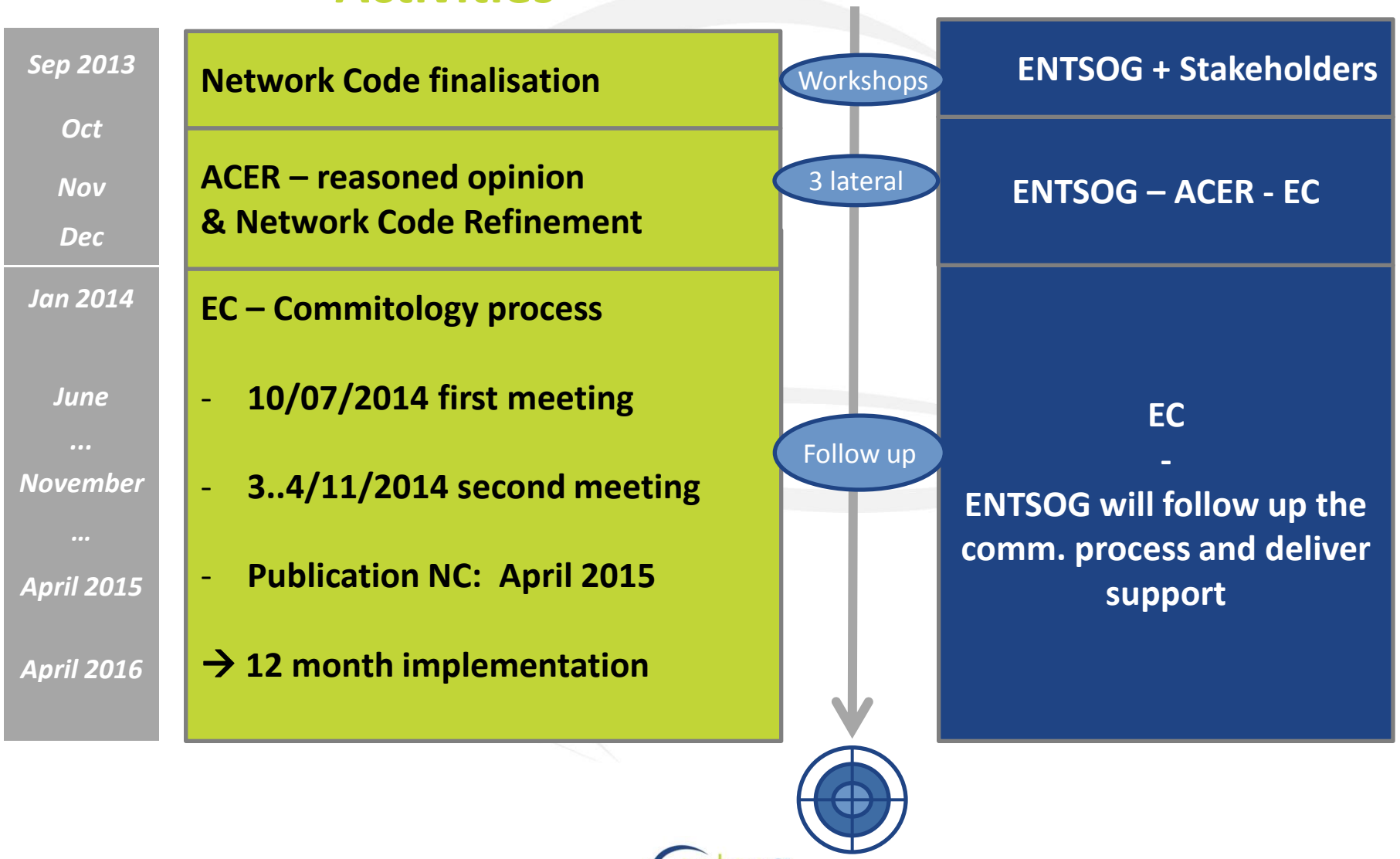
- **CNOT:**
  - shall specify common DE solution for respective requirement
  - may include: Business Requirements Specifications (BRS), release management and implementation guidelines
  - shall be **published on ENTSOG website**

- **CNOT process:**
  - ENTSOG shall establish transparent process for CNOT development
  - ENTSOG shall conduct a consultation for each CNOT

→ Currently CNOTs for Capacity booking process and Nominations and Matching process

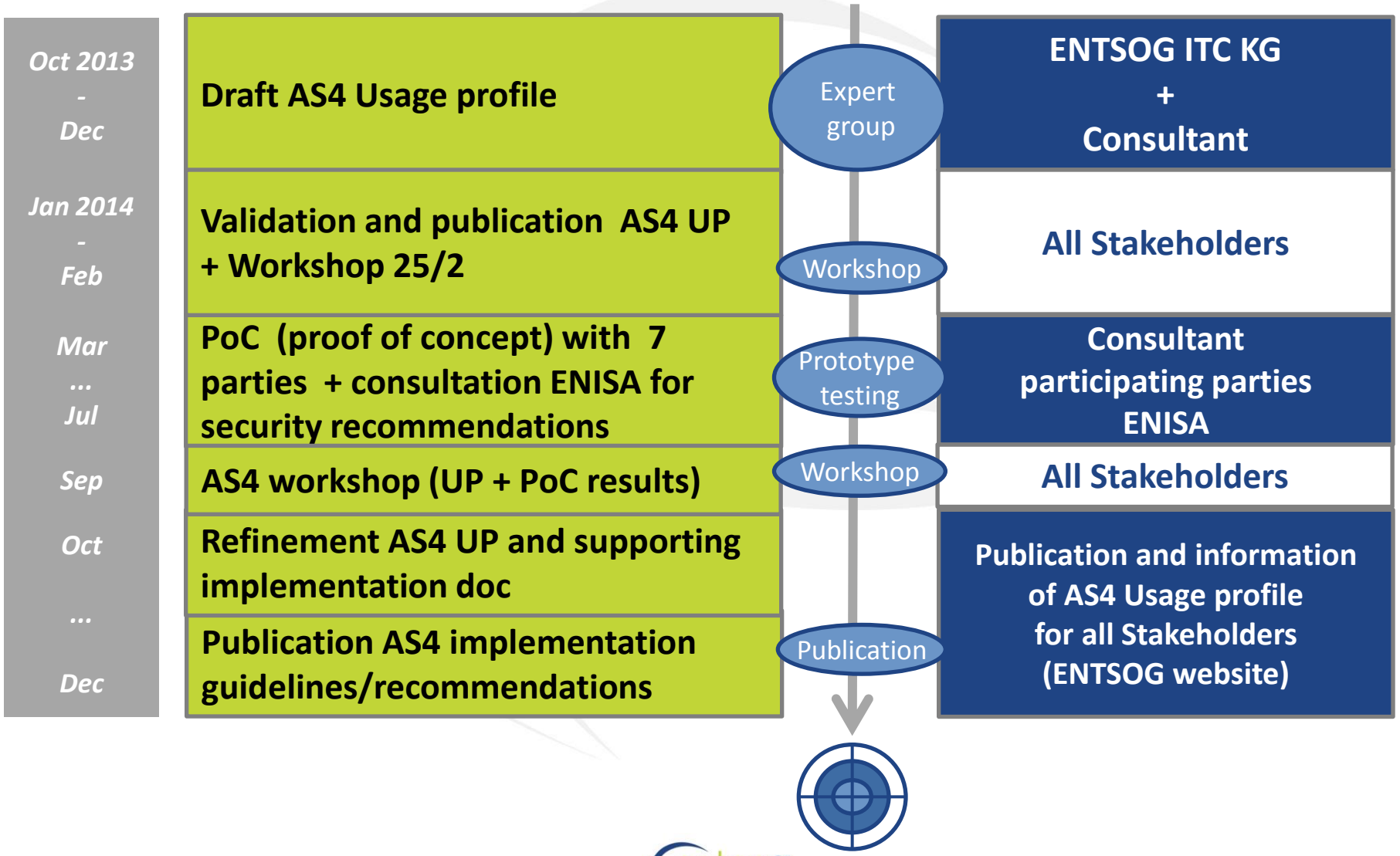
INT NC Status

Activities

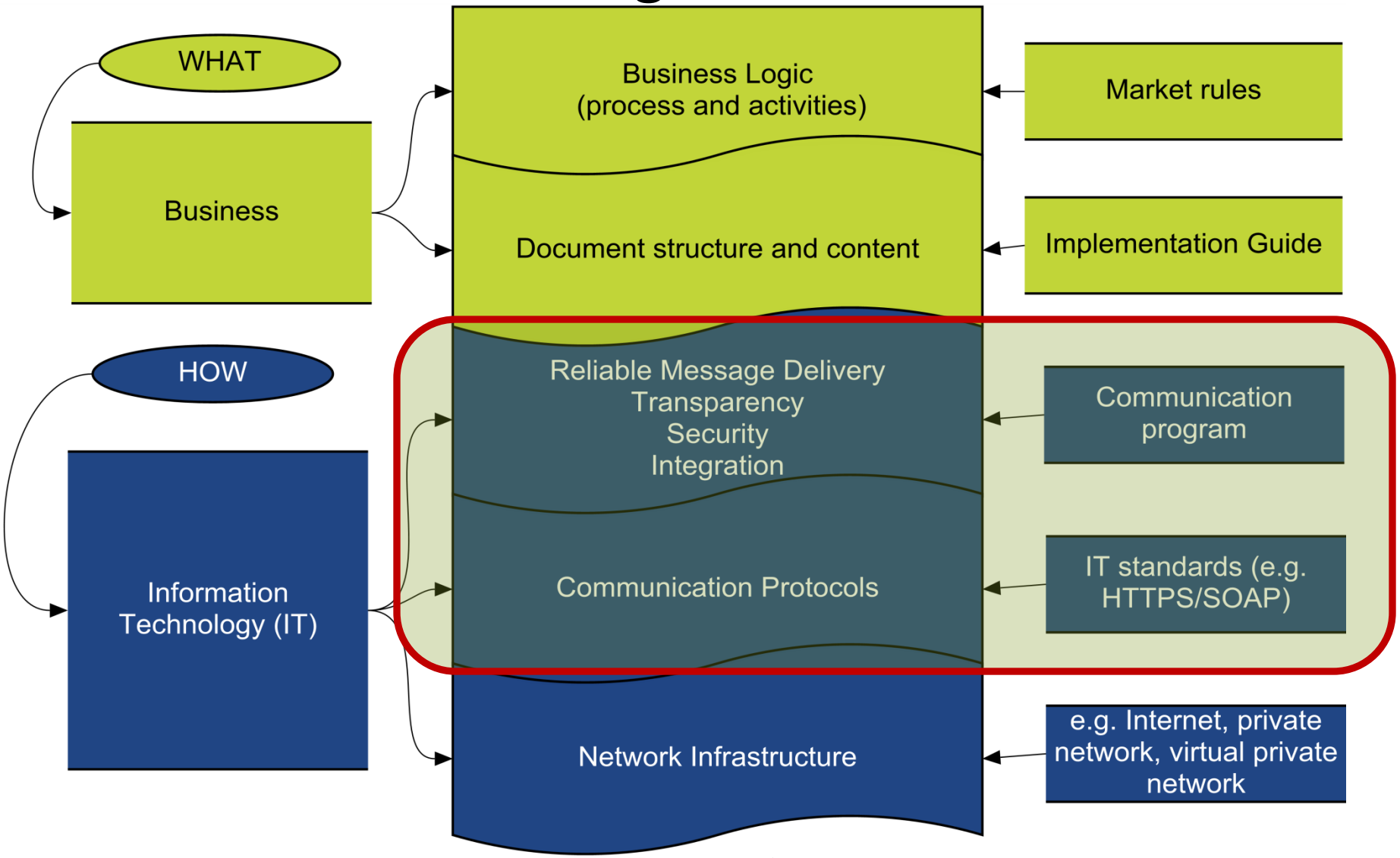


INTRODUCTION
-
AS4 Development

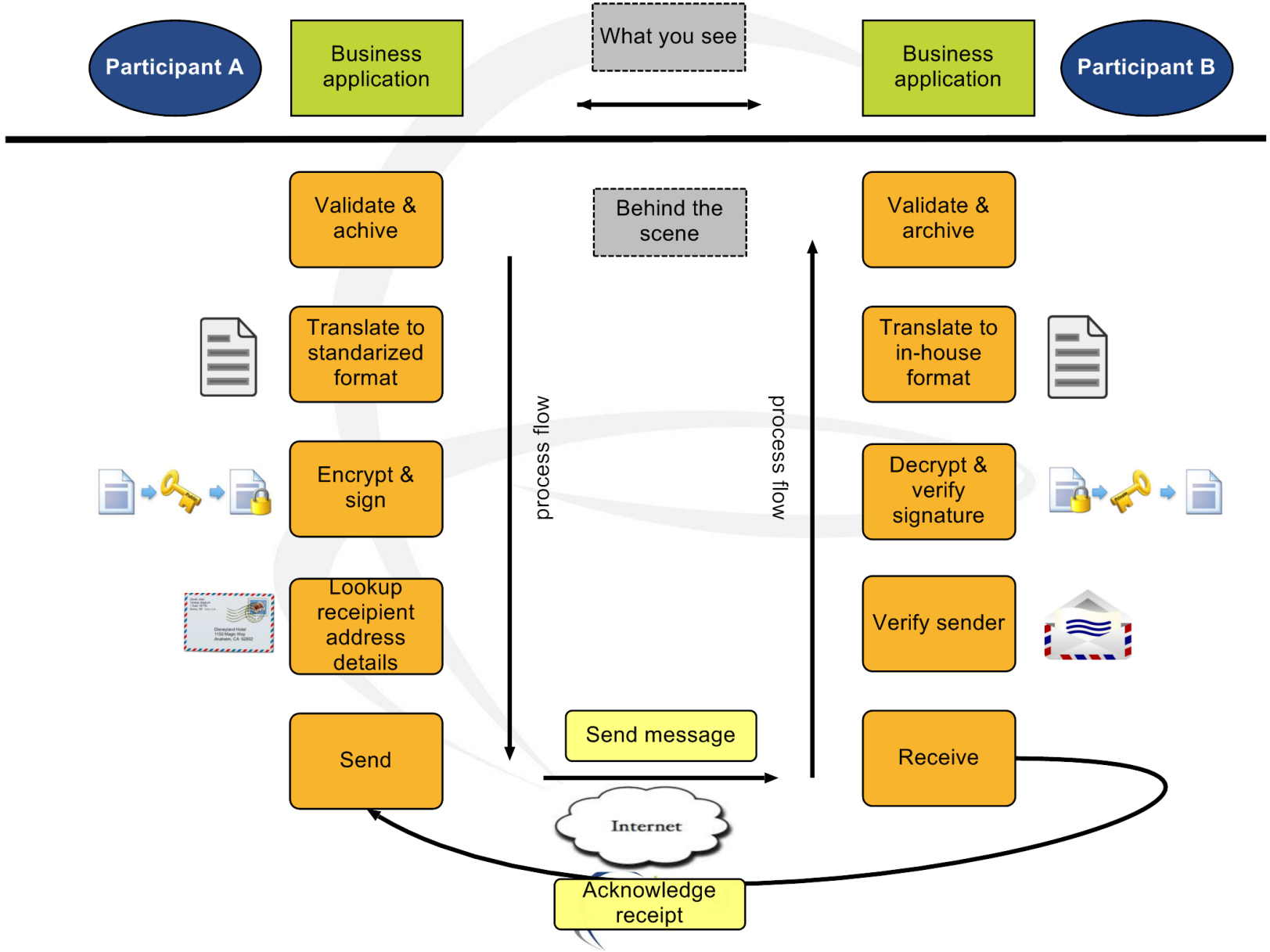
AS4 Development Process



Data Exchange – What & How



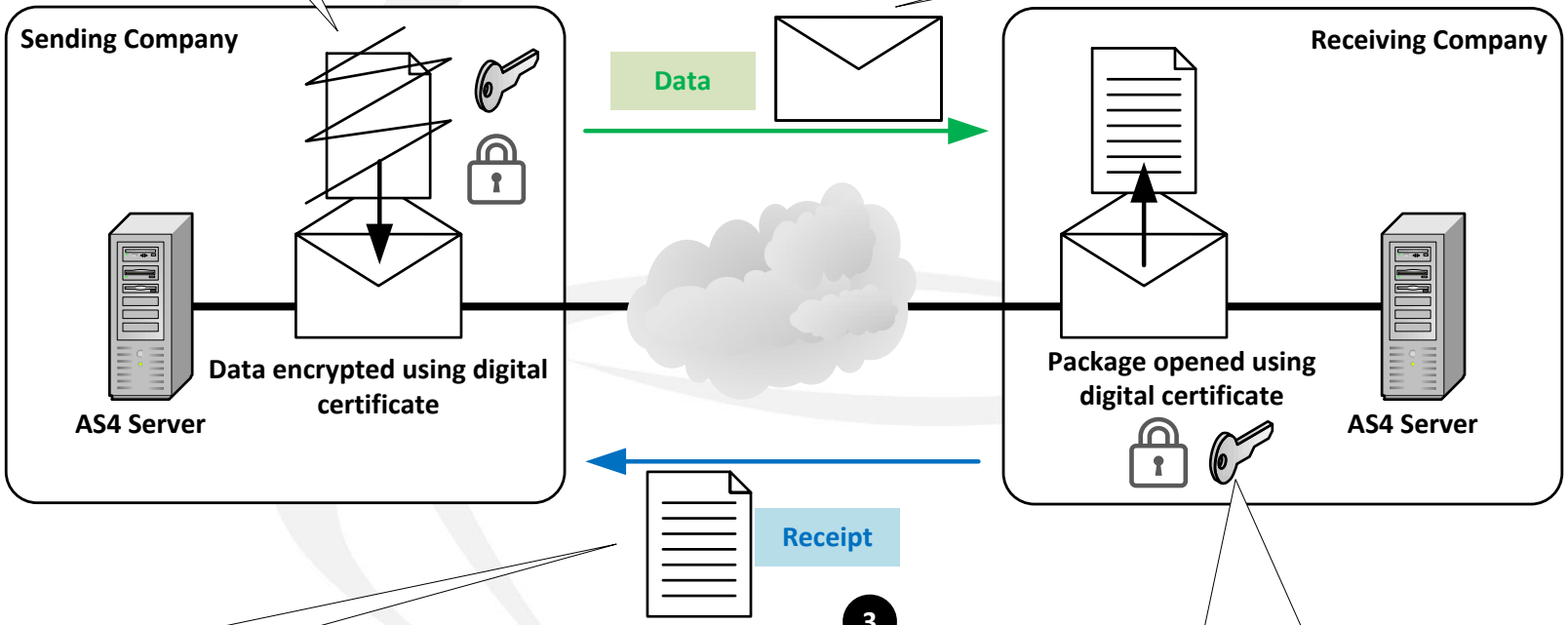
End-User Perspective



Communication Perspective

1 An AS4 server uses a digital certificate to encrypt a business document that has been digitally signed.

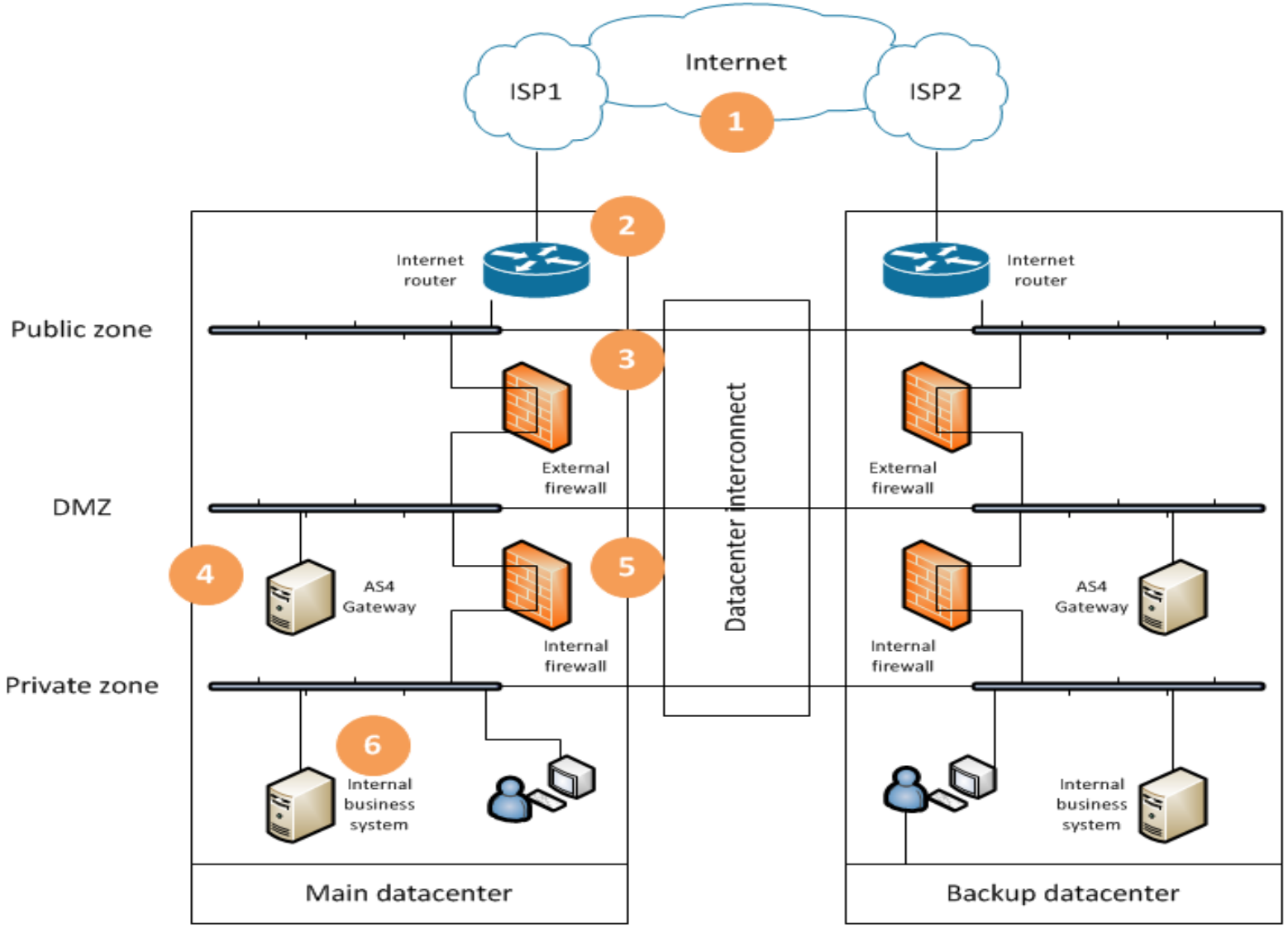
2 The server sends the document over an IP network to the AS4 server at the receiving company.



4 The receiving server sends a receipt message to the sending server.

3 The AS4 server confirms the digital signature and decrypts the data using the digital certificate.

System Perspective (1)



System Perspective (2)

1. Internet access should be split over two or more Internet Service Providers to deliver high availability on the internet connectivity. The internet accesses should be distrubuted over the available datacenters to optimize geographical redundancy and avoid a "single source of failure".

2. On premise internet routers capable of rerouting traffic to and from the internet in case of failure on the internet lines. These will typically handle fail over scenario's between the datacenters.

3. External firewalls to be able to filter internet traffic for specific 'allowed' communication. This is the first defence barrier to the Demilitarized Zone.

4. Typically the AS4 protocol will be handled by a gateway residing in the DMZ. This is the point where the AS4 protocol ends. The webservices/ SOAP engine will be hosted on this device.

5. Second security barrier: the internal firewall. This device will filter only the protocol needed between the front AS4 gateway and the internal business system. This will be implementation specific.

6. The internal business system as the endpoint for the business communication. Through this system users get access to the documents that were exchanged by the AS4 handlers.

WHAT IS AS4

Pim van der Eijk

B2B Integration

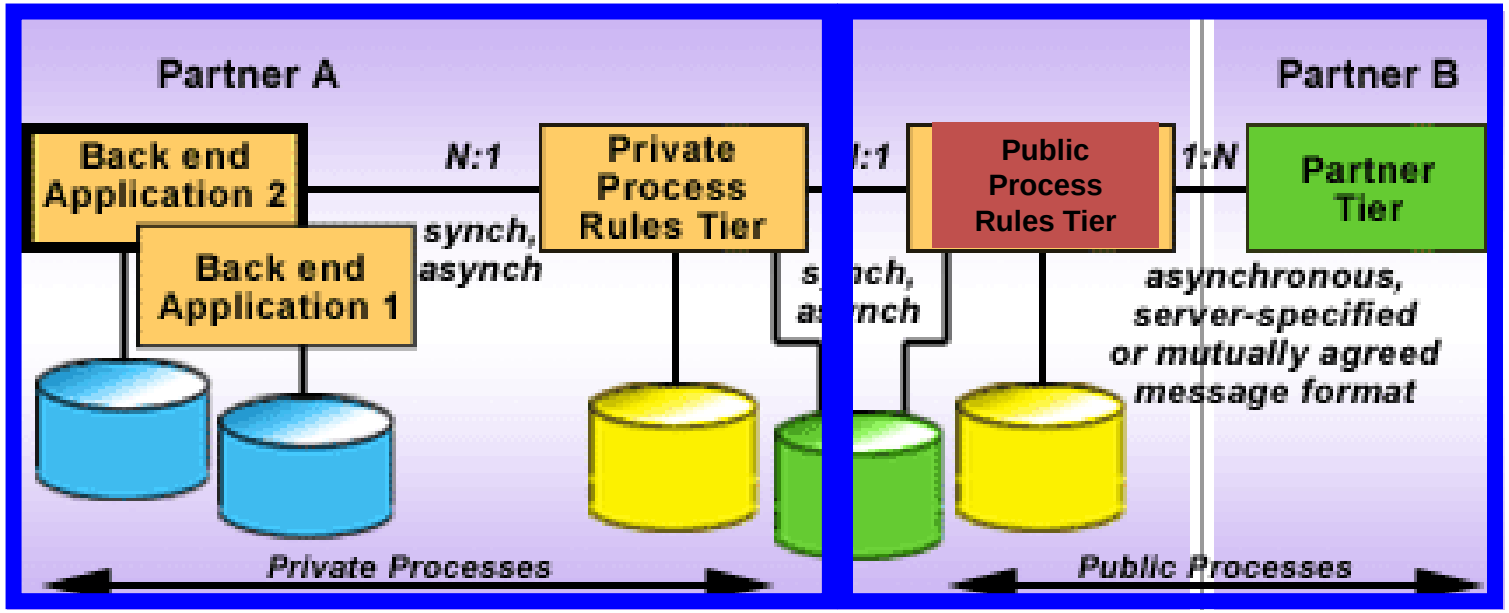
Document-based B2B:

- Organizations **synchronize** their **business processes** at specific agreed process steps
- Synchronization involves exchange of information as **structured documents**
- Information produced and consumed by **business applications**
- **Standardized structure** and format of content (EASEE-gas XML schemas)

Complementary to other exchange paradigms

- Portal-based communication allows end-users to access remote functionality (interactive Data Exchange)
- Direct communication allows partner application to invoke remote application functionality (integrated Data Exchange)

B2B Architecture



Enterprise Application Integration, Workflow Management

Participation in e-business (e-Government) collaborations

IBM Patterns for e-Business http://www-106.ibm.com/developerworks/patterns/

B2B Requirements

- **Support fully automatic processing**
  - **Structured** business **content**
  - Structured **metadata** to express purpose and requested processing
- **Security**
  - **Protect integrity** and **confidentiality** of content
  - **Authenticate** identity of sender and receiver
- **Reliability**
  - **Guaranteed** once-and-only once delivery
- **Open Standard**
  - Mechanism should be **independent** of specific vendor products
  - TSOs should be able to procure solutions in a competitive environment

ebXML

Technical and semantic interoperability

Modular, cohesive set of B2B standards developed from 1999

- OASIS, ISO and UN/CEFACT
- ISO 15000 standards since 2004

> **OASIS ebXML standards support**

- Secure reliable messaging, rich metadata
- Choreographed business collaborations
- Partner agreements and management
- Registry functionality

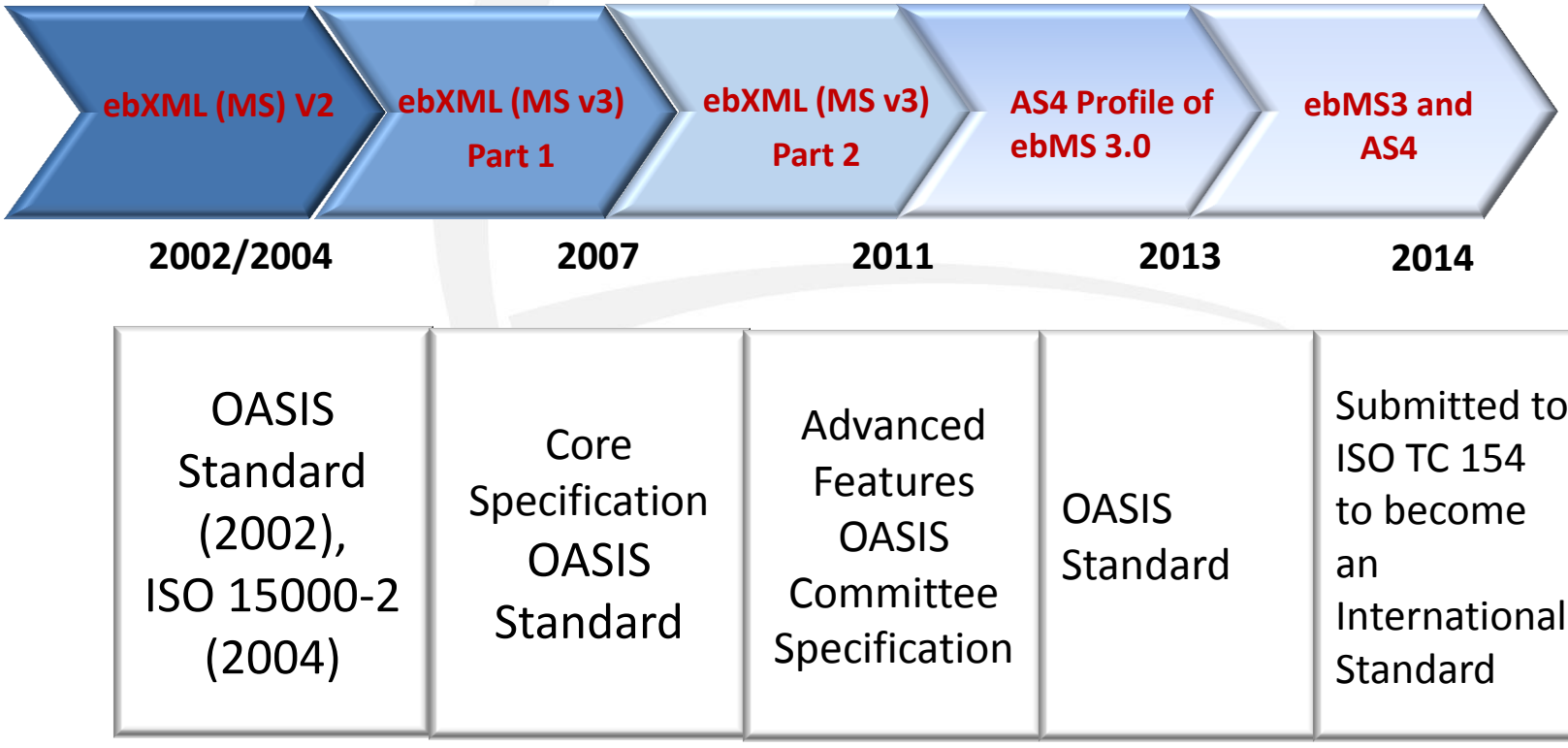
One component is ebXML Messaging (ebMS)

ebXML - High Level Capabilities

- **Message Header with Business Metadata**
  - Identifies Business Partners, Transaction Semantics, Context, Agreement, Properties, Payloads
- **Reliable Message Delivery**
  - At-Least-Once, At-Most-Once, In-Order delivery
- **Secure Messaging**
  - Digital Signature and Payload Encryption
  - Support for Non-Repudiation of Origin & Receipt
- **Flexible Packaging using SOAP and MIME**
  - XML, EDI, multimedia payloads
  - Multiple payloads per message
- **Transport Protocol Mappings**
  - HTTP and SMTP

ebXML Messaging Standards

History and evolution of AS4



ebXML Messaging Standards

B2B exchange protocol based on Web Services

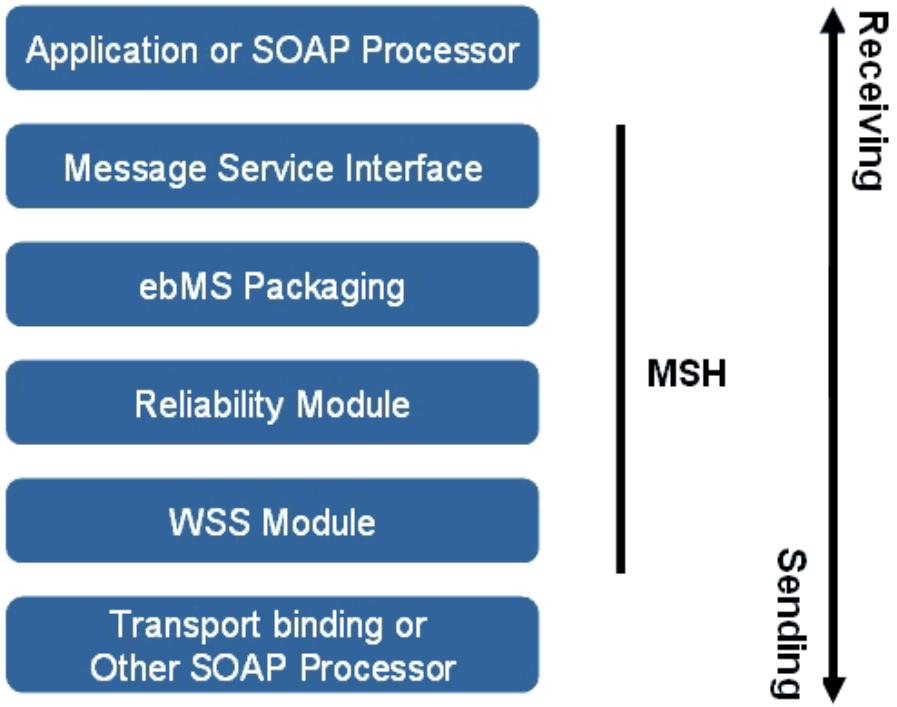
B2B header and envelope

SOAP, WS-Security

Reliable Messaging

"Processing modes" for configuration

Push and Pull



AS4 – an interoperable profile

- **Functionally similar to older standards, but**
  - Based on more modern **Web Services** technology
  - Provides enhancements for SMEs (client only endpoints)

- **Profile ebMS 3.0 by**
  - **Reducing options** and filling in details (e.g. for Receipts)
  - Not using modules with known complexity and interoperability issues, e.g. WS-ReliableMessaging
  - Adding some AS2-like features (e.g. compression)

- **Three Conformance Profiles**
  - Subsets mapping to classes of product implementations

THE AS4 PROFILE FOR TSOs

Objectives

- Support exchange of EDIG@S-XML documents and other payloads.
- Support business processes in the gas sector
- Leverage experience gained with other B2B protocols, such as AS2 as described in the EASEE-gas implementation guide.
- Provide security guidance based on state-of-the-art best practices, following recommendations for “near term” (defined as “at least ten years”) future system use.
- Provide suppliers of AS4-enabled B2B communication solutions with guidance regarding the required AS4 functionality.

Profiling AS4

>Selecting an AS4 Conformance Profile

- AS4 defines three “Conformance Profiles”
- ENTSOG profile is based on “ebHandler”

>Profiling the ebHandler Feature Set

- Following the structure of ebMS 3.0 Core
- Detailed information for product vendors and for production selection

>Defining a Usage Profile

- Guidance for implementation and operation teams at TSOs

AS4 Conformance Profiles

- Selection of ebHandler Conformance Profile
- Feature review of ebHandler Conformance Profile
- Usage Profile

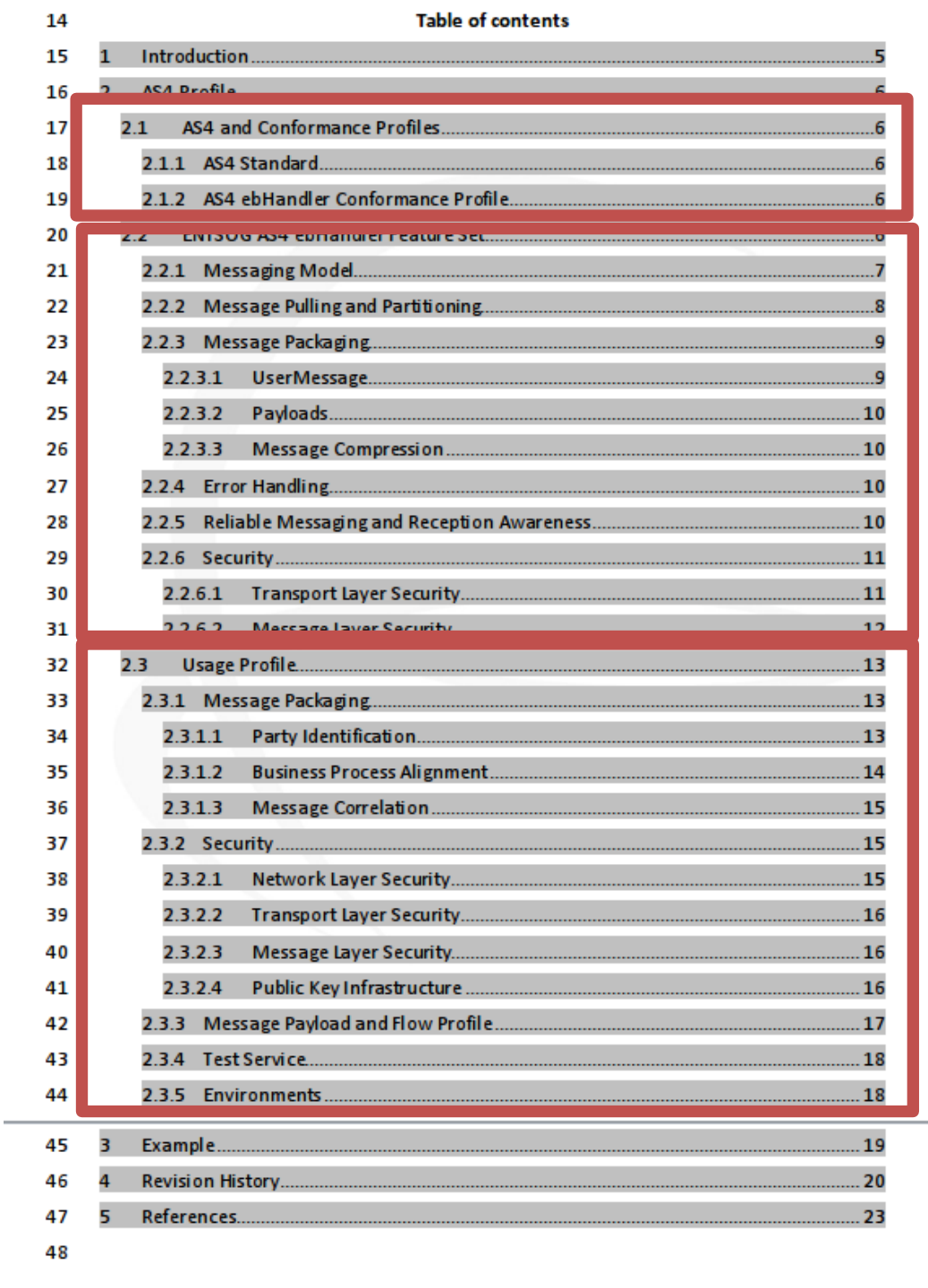
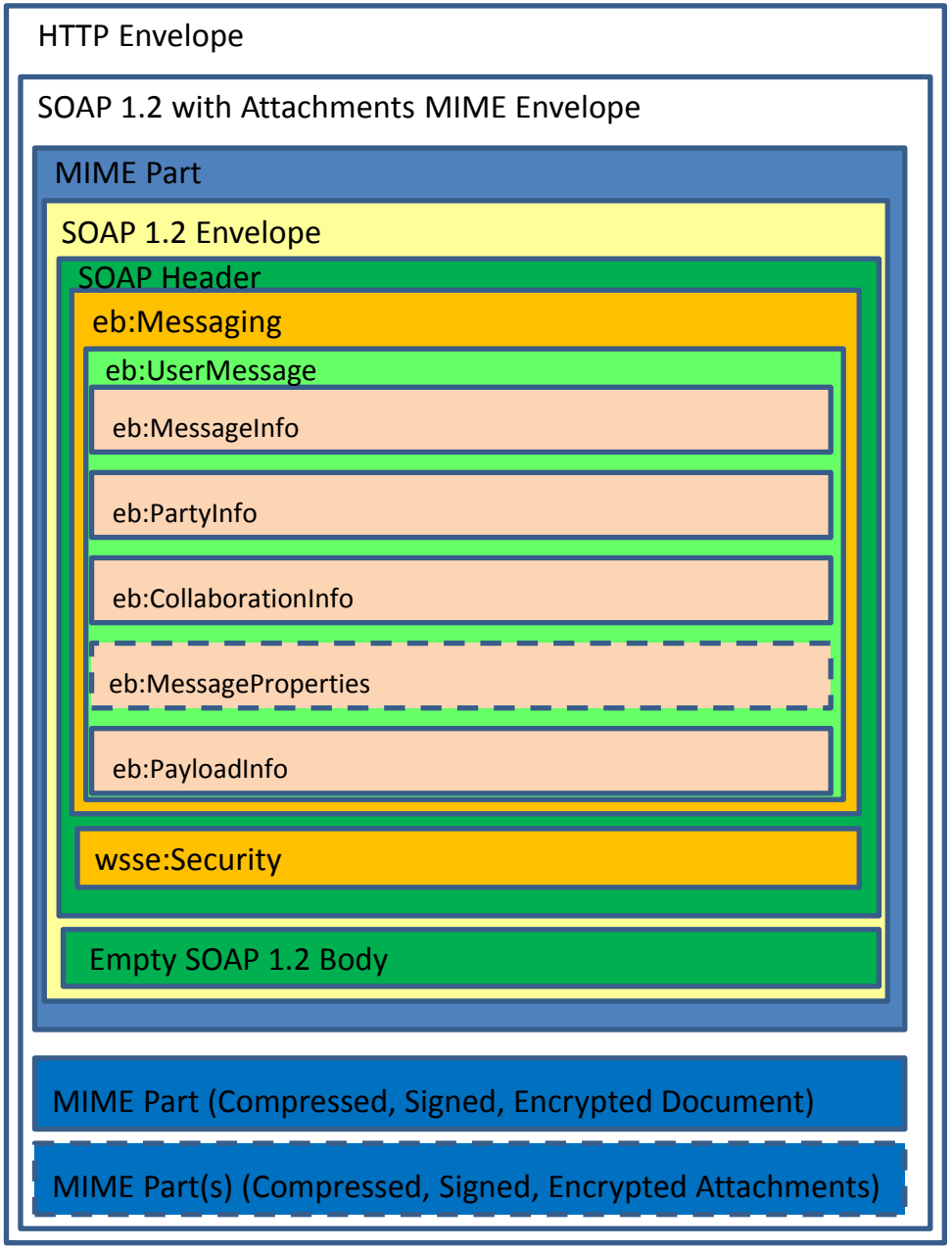


Table of contents

ebMS 3.0 Packaging

- **AS4:**
  - SOAP 1.2 with Attachments
  - SOAP Header with Messaging extension headers
- **ENTSOG Profile:**
  - No content in SOAP Body
  - Main business document in separate MIME part
  - Optional adjunct payloads
  - All payloads compressed, signed and encrypted



SECURITY IN THE ENTSOG PROFILE

Security

>Aspects

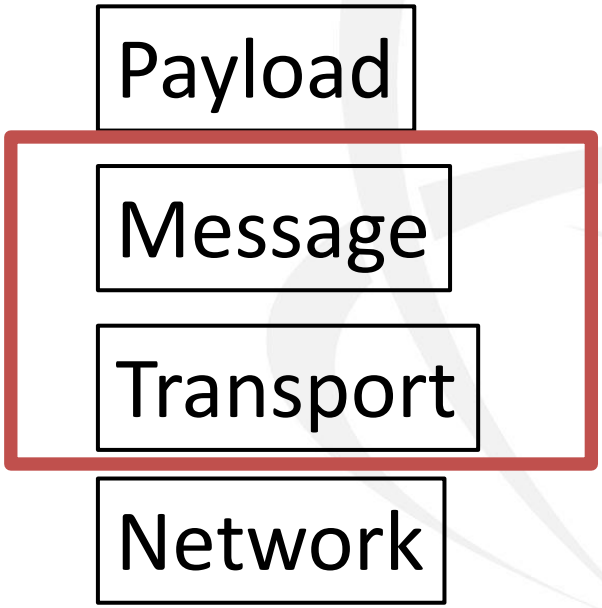
- Authentication of Sender (Client)
- Authentication of Recipient (Server)
- Authorization
- Confidentiality of Content
- Non-Repudiation of Origin and Receipt

>Layers

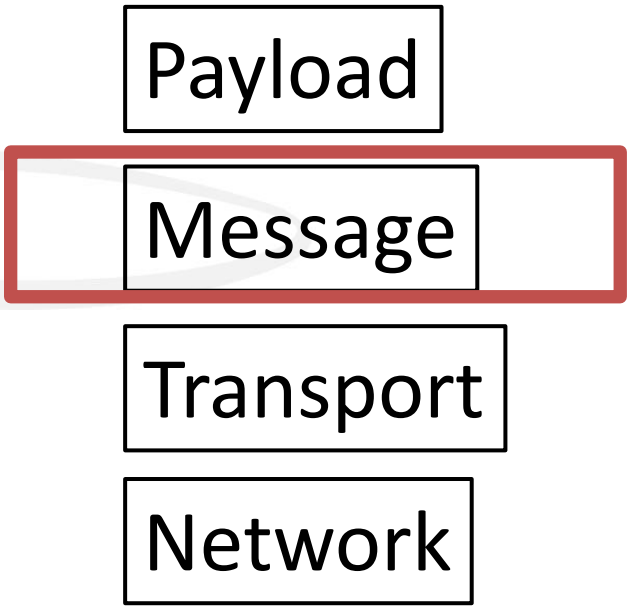
- Network Layer (VPN)
- Transport Layer Security (SSL, TLS)
- Message Layer using WS-Security
- Payload Layer (application-generated)

Security Layers for B2B Gateway

- TLS handled by B2B product (Product Feature)



- TLS offloaded (Deployment Option)



TLS Configuration

>Guidance

- Algorithms, Key Sizes and Parameters Report 2013 recommendations version 1.0 – October 2013. ENISA
- Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG für den Einsatz des SSL/TLS-Protokolls in der Bundesverwaltung. Bundesamt für Sicherheit in der Informationstechnik (BSI)

>Transport Layer Security

- TLS Version: 1.2 recommended
- Cipher Suites: Perfect Forward Secrecy (PFS) supported by TLS_ECDHE_* and TLS_DHE_* cipher suites
- ENISA recommends only 8 encryption modes (*_WITH_AES_128_GCM_SHA256 and 7 others)

>Client authentication as deployment option

WS-Security

- **Latest version is WS-Security 1.1.1**
  - http://docs.oasis-open.org/wss-m/wss/v1.1.1/
- **Message Signing**
  - Uses W3C XML Security and underlying algorithms
  - http://www.w3.org/TR/2013/REC-xmldsig-core1-20130411/
- **Message Encryption**
  - Uses W3C XML Encryption and underlying algorithms
  - http://www.w3.org/TR/2013/REC-xmlenc-core1-20130411/
- **XML Security for**
  - SOAP headers (ebMS header signed, not encrypted)
  - SOAP body
  - MIME payload parts
  - Signals (Errors and Receipts)

WS-Security Guidance

Signing

- Recent updated version of XML Signature
- Digests are to be computed using SHA256
- Signatures to be computed using RSA-SHA256

Encryption

- Based on W3C XML Encryption
- Content to be encrypted using AES-128-GCM

Non-Repudiation

Non-Repudiation of Origin

- Commits sender to content of message
- Implemented using WS-Security Signature
- SignedInfo includes identifiers and digests of payload parts and ebMS header

Non-Repudiation of Receipt

- AS4 NRR echoes the SignedInfo of received message
  - Validated by receiving WS-Security module
  - NRR receipt is itself signed by Recipient
  - AS4 Receipt is sent once all MSH processing has completed

NRO and NRR assume storage of non-repudiation data

Authorization

Partner management

- Access Control based on configuration in B2B product

Processing modes

- Control over types of messages accepted from particular trading partners

AS4 Vendors

AS4 – Vendors

- ADES
  - http://www.ades.at/
- Applied Technologies
  - http://www.appliedtechnologies.de/Loesungen/Pages/Was_ist_AS4.aspx
- Axway
  - http://www.drummondgroup.com/index.php/b2b-certified-products/certified-products/as4
- Bosch Inubit
  - https://www.bosch-si.com/de/loesungen/energie/marktkommunikation/marktkommunikation.html?ref=ga-inst-2014h1-brand-brand-de
- DICentral
  - http://diconnect.portal.dicentral.com/Pages/Product/AS4-EDI.aspx
- Flame
  - http://flame.co.za/?page_id=14

AS4 – Vendors

- IBM
  - http://www-03.ibm.com/software/products/en/b2b-integrator
- Oracle
  - Upcoming as patch to Oracle SOA Suite 12.1.3.
- Ponton
  - http://ponton.de/index.php?option=com_content&view=article&id=32%3Aponton-erweitert-sein-produkt-ponton-xp-um-das-protokoll-as4&catid=7%3Anews&Itemid=2&lang=en
- Seeburger AG
  - http://www.seeburger.com/home.html
- Software AG
  - http://www.softwareag.com/corporate/products/wm/integration/products/b2b/capabilities/default.asp
- Tibco
  - https://docs.tibco.com/pub/businessconnect_ebxml_protocol/6.0.1_july_2013/pdf/tib_bcebxml_user_guide_ebMS3.pdf

AS4 – Vendors (Australia)

- Fujitsu
  - http://www.fujitsu.com/au/products/software/middleware/business/xbrl/
- GBST
  - http://gbst.com/our-expertise/wealth-management/superstream-solutions
- IQGroup
  - http://www.iqgroup.com.au/services/solutions/iqsuperstream/
- OBAN
  - http://www.obansolutions.com.au/

Questions

SuperStream project

AXWAY

AS4 for SuperStream

Antoine Rizk

Axway

Brussels– September 2014

Agenda

- The Australian SuperStream initiative
- Comparison with ENTSOG AS4 profile
- SuperChoice experience with Axway
- Conclusions/Questions

© 2013 Axway | Confidential

axway
business. in motion.

The Australian SuperStream initiative

SuperStream

- SuperStream is an Australian Federal Government program designed to improve the efficiency and reduce the cost of superannuation processing by up to A$1 billion per year.

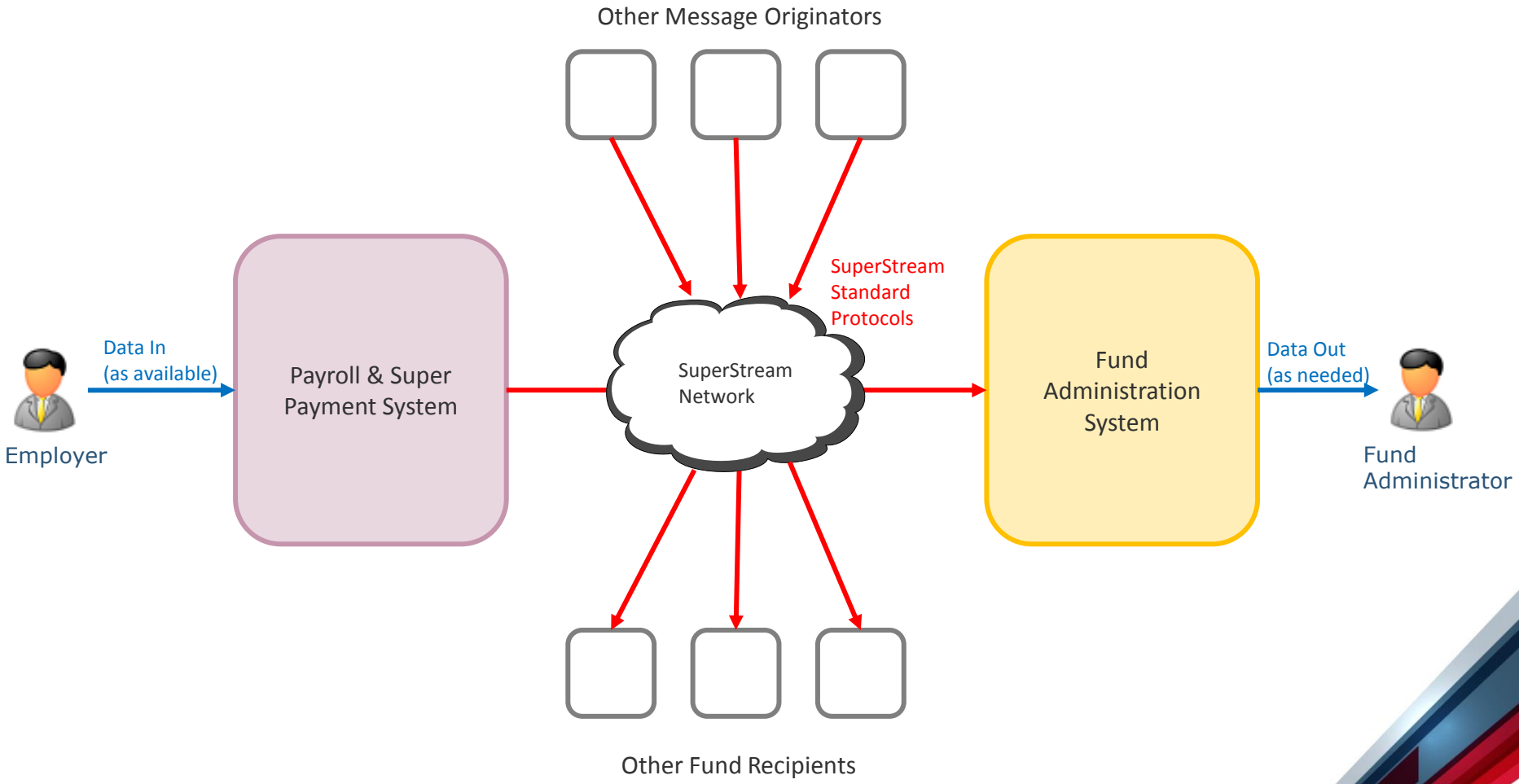
- Under subsection 34K(3) of the Superannuation Industry (Supervision) Act 1993 (SISA 1993), the legislation mandates that employers and trustees of superannuation entities use a new communications standard (ebMS v3 with AS4 profiles) and standardized XBRL document structures for rollover transactions and superannuation contributions.

- A network of gateways, the Superannuation Data and Gateway Service Standards, has been established to facilitate the implementation of SuperStream.

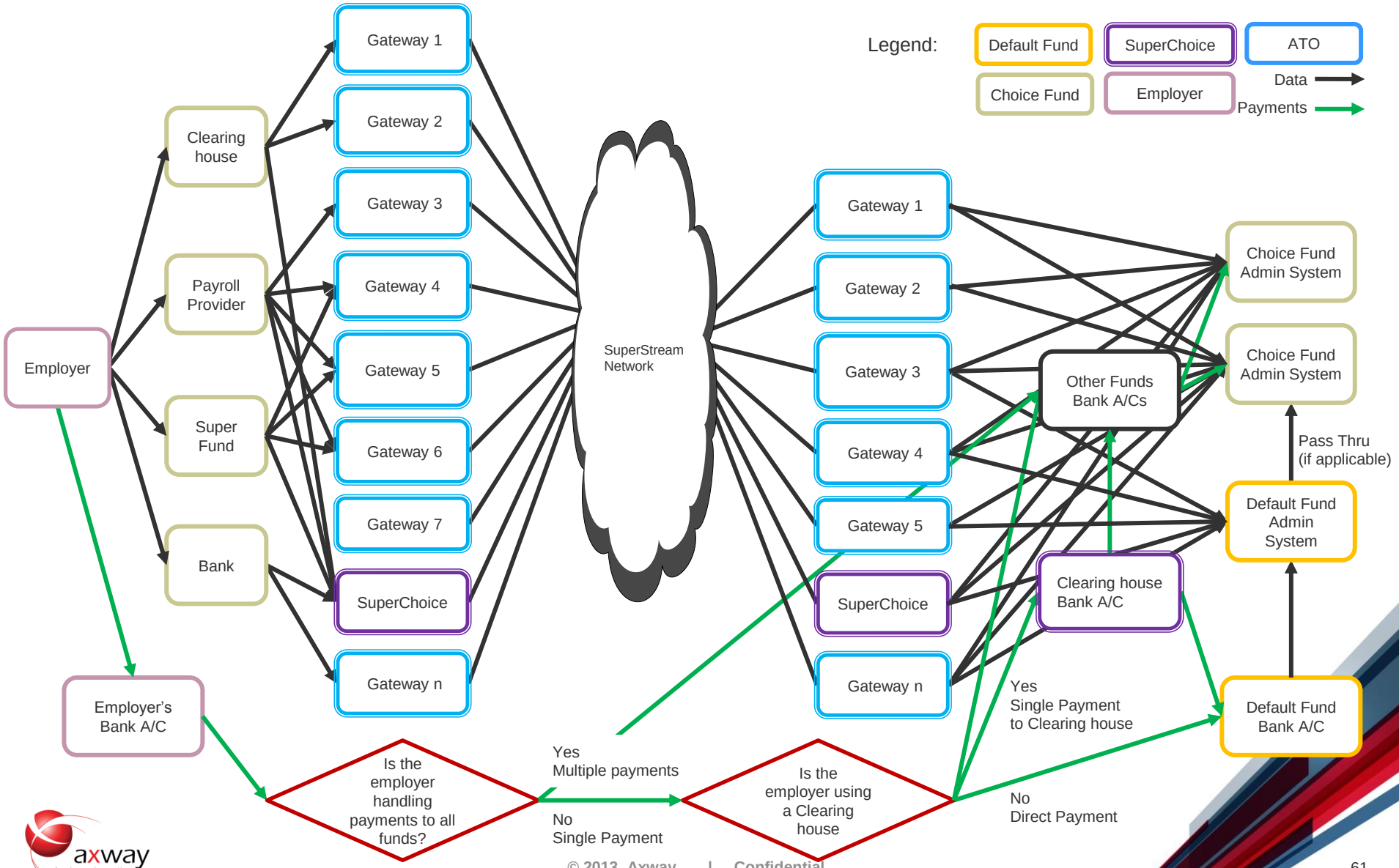
- Using the gateway network, employers and funds will be able to exchange information through one channel, rather than directly with approximately 350 individual funds.

© 2013 Axway | Confidential

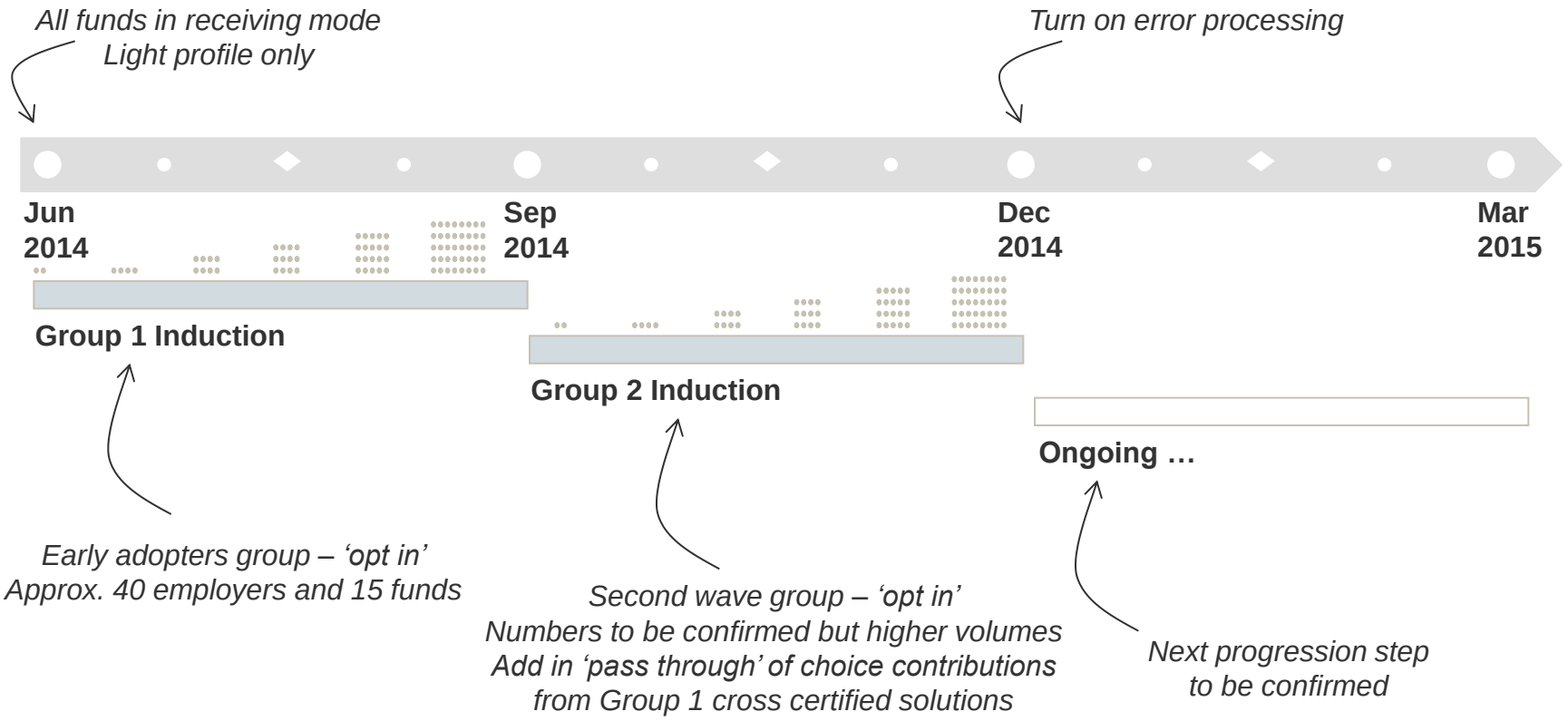
Simplified View of Contributions Under SuperStream



Realistic view of Contributions under SuperStream



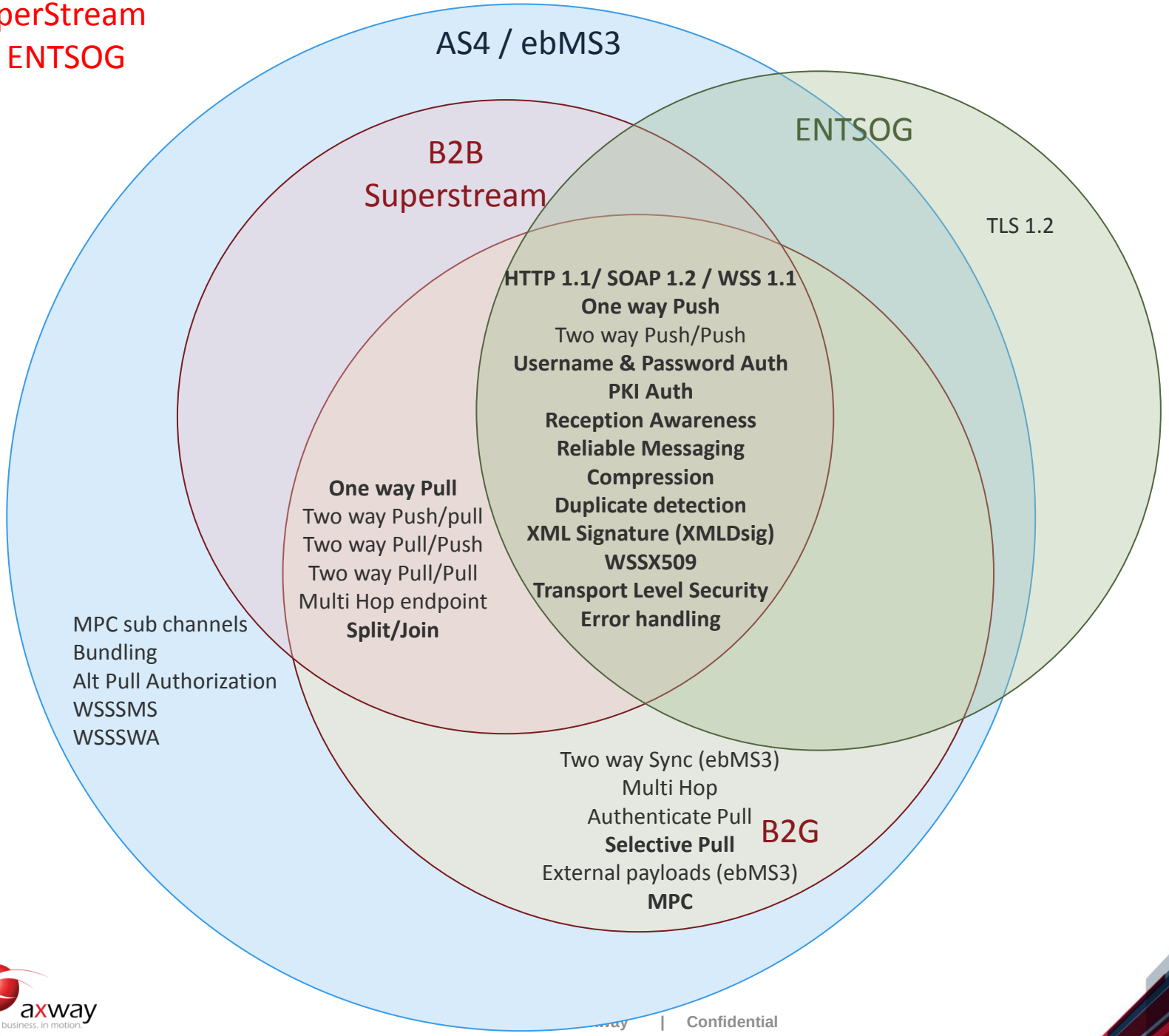
Transition Timetable for 2014-5



Source: ATO Contributions Working Group Presentation 2013-12-10

SuperStream – ENTSOG AS4 Profiles

SuperStream vs. ENTSOG



SuperStream Profiles (1/2)

Profile	Ultra-Light	Light	High-End	Large Volume	Application Gateway
Send with receipt of transmission errors	Yes (one-way push)	Yes (one-way push)	Yes (one-way push)	Yes (one-way push)	Yes (one-way push)
Receive (e.g. error messages)	No (no need for one-way pull)	Yes (one-way pull)	Yes (one-way push or pull)	Yes (one-way push or pull)	Yes (one-way push and one-way pull)
Permanent internet presence	No	No	Yes (if using one-way push)	Yes (if using one-way push)	Yes
Support for one-way pull as responder	No	No	No	No	Yes
Automated business error messaging	No	Yes	Yes	Yes	Yes

© 2013 Axway | Confidential

SuperStream Profiles (2/2)

Profile	Ultra-Light	Light	High-End	Large Volume	Application Gateway
Username Token based security	Yes	Yes	Yes	Yes	Yes
Digital signatures and encryption	No	No	Yes (optional)	Yes (optional)	Yes (must be used for g/w←→g/w
Reliable Messaging	Yes	Yes	Yes	Yes	Yes
Compression-enabled	No (<20 MB)	No (<20 MB)	Yes	Yes	Yes
Large Message Splitting and Joining	No (< 1GB)	No (< 1GB)	No (< 1GB)	Yes	Yes
Multi-hop	As a Client	As a Client	As a Client	As a Client	Yes
Standard AS4 Profile Conformance	AS4 Light Client	AS4 Light Client	AS4 ebHandler	AS4 ebHandler	AS4 ebHandler

© 2013 Axway | Confidential

SuperChoice Case Study

© 2014 Axway

Who is SuperChoice

SuperChoice …

- Is Australia's leading superannuation eCommerce exchange / clearing house
- Has been operating for over 15 years
- Provides online contribution processing systems to over 40% of Australia's largest pension providers
- Handles contributions to over 100,000 employers on behalf of nearly 3 million employees
- Handles nearly 20% of all contribution payments to active SMSFs
- Handles an estimated 50% of all electronic employer superannuation contributions
- Entered the UK pensions market in 2012

Axway …

- Is a software company focussed solely on "Governing the flow of data"
  - Manages interactions and integrations between applications, people and communities
- Has offices in 18 countries including Australia; $314 M revenue in 2012
- Has over 11,000 customers across 100 countries with 120+ Australian customers:
  - 14 of the top 25 Global Banks, 5 of the top 6 US Banks
  - 9 of the top 20 container ports
  - 17 of the top 24 global auto parts suppliers

© 2014 Axway

Key challenges with SuperStream Contributions

Key challenges for participants:

- Managing the significantly greater complexity involved:
  - Employers are not homogeneous
  - Lots more participants
  - Less engaged; less IT support
- Making progress while resolving the regulatory and operational uncertainty
- Increasing security requirements; its not the dollars, its your identity they are after!
- Dealing with more new entrants
- Increasing difficulty of diagnosing issues; more so than Rollovers

© 2014 Axway

Employers are not homogenous

Employer Characteristics:

- 69.2% of employers pay Contributions by electronic transaction and cheque
- 91.9% of all employers have access to the internet
- 24% of all employers have no IT support staff
- Not all employers have a single Default Superannuation Fund:
  - 65% have one Default fund
  - 18% have 2 Default funds
  - 5% have more than 5 Default funds
  - 78.9% have more than 10 Choice funds
- Not all employers have an ABN or a single payroll system or know too much about SuperStream!

Source: Rice Warner Nov 2011; ABS Cat 8129.0, released 22/08/2013; NSW Business Chamber, Dec 2013

© 2014 Axway

Developing a pilot AS4 / ebMS solution was invaluable

- **Developed a pilot AS4 / ebMSv3 solution based on the Holodeck open source kernel:**
  - Get operating in our environment
  - Build out functionality:
    - Support SuperStream requirements
    - Operationalise
- **Learnt a lot from the pilot:**
  - Hard to understand how Holodeck worked
  - No local / few international sources of Holodeck or AS4 / ebMS expertise
  - Few vendors supported AS4 / ebMSv3, mostly “promises of things to come”
  - High delivery risk:
    - Estimates to build out functionality were way too low
    - Delivery timeframes too long / uncertain
- **Decided to undertake in tandem a third party option as a backup strategy:**
  - Leverage proven AS4 / ebMS expertise of a dedicated B2B communications player

© 2014 Axway

Lessons Learned from SuperStream Rollovers experience

Key Lessons:

- SuperStream standards aren't homogeneous; variations in interpretation did occur
- Gateway interoperability testing took much longer than expected
- Java was a good choice for the Gateway; its hard to get Microsoft to change anything
- Superannuation Transaction Network Working Group worked well to ensure Rollovers worked
- There's value in engaging early:
  - The better prepared; the fewer issues experienced
  - Long tail of less prepared players resulted in lots of support required
- It's a scale activity so you need to be very clear about your business case

© 2014 Axway

Selecting Axway achieved real, tangible benefits

Benefits from using Axway:

- Lowered the implementation risk and cost
- Leveraged the framework B2Bi provides, such as the DMZ-router
- Provided significant admin / operational support capability uplift
- Provided the ability to leverage benefits to the existing bespoke solutions
- Obtained Drummond certification
- Provided on-going new functionality and capability updates

Viable options exist for communicating under SuperStream

© 2014 Axway

Thank you

 © 2013 Axway | All rights reserved.

Questions

Coffee

11.45--12.00

“Lessons learned”

EASEE-gas
Wim de Olde

ENTSOG AS4 Workshop

DIGITAL SECURITY CERTIFICATES LESSONS LEARNED

Wim de Olde
TSWG, EASEE-gas

Definitions

- The transport protocol supports cross-enterprise collaboration using secure and reliable exchange of business documents.
- AS2 and AS4 are transport protocols using existing standards
  - Content independent
  - Business information independent
  - Can be used secure using certificates
- Certificates are used to:
  1. Identify a company (preferably not systems)
  2. Encrypt and sign content which is transported
- Server certificates
  - Server Certificates are used to identify a server. Typically they are issued to hostnames or web addresses like “b2b.company.com”. These certificates are used to encrypt the connection (TLS/SSL-> Https). Out of scope.
- Self signed/created certificates
  - Not allowed

EASEE-gas & AS2 facts

- September 2007 EASEE-gas CBP for the use of AS2 over Internet
  - Migration from ISDN/FTP and X.25
- Selection single certificate provider for EASEE-gas certificates
  - DigiNotar, now QuoVadis
- Procedures
  - New/Renew Certificates
  - Revoke Certificate
  - Periodical Renewal of Certificates
  - Request Certificate
- AS2 implementation guide
  - Common, not implementation specific
- Currently approx. 62 companies using AS2 and certificates
- Nomination process: Availability – Confidentiality - Integrity

Certificates

- Why specific certificates for B2B communication?
  - Part of the procedure: check if company is eligible to join gas market communication
  - Specific fields in the certificate, e.g. EIC code
    - Checked by certificate provider before issuing the certificate
    - Perform mapping in communication software
  - One trusted third party, mutually agreed
    - No need to check trustworthiness in contradiction to unknown (local) certificate providers
  - One validity chain (root certificates)
    - Security policies often demand that the standard list of trusted root certificates is empty; only root certificates are used which are present in the communication software.
  - Orchestrated change of certificates
    - Pro: One planned change which can be prepared and tested
    - Con: Central project/organisation needed, fixed date for the change

Security: Limit the amount of possible valid certificates

Easier in operations

Security

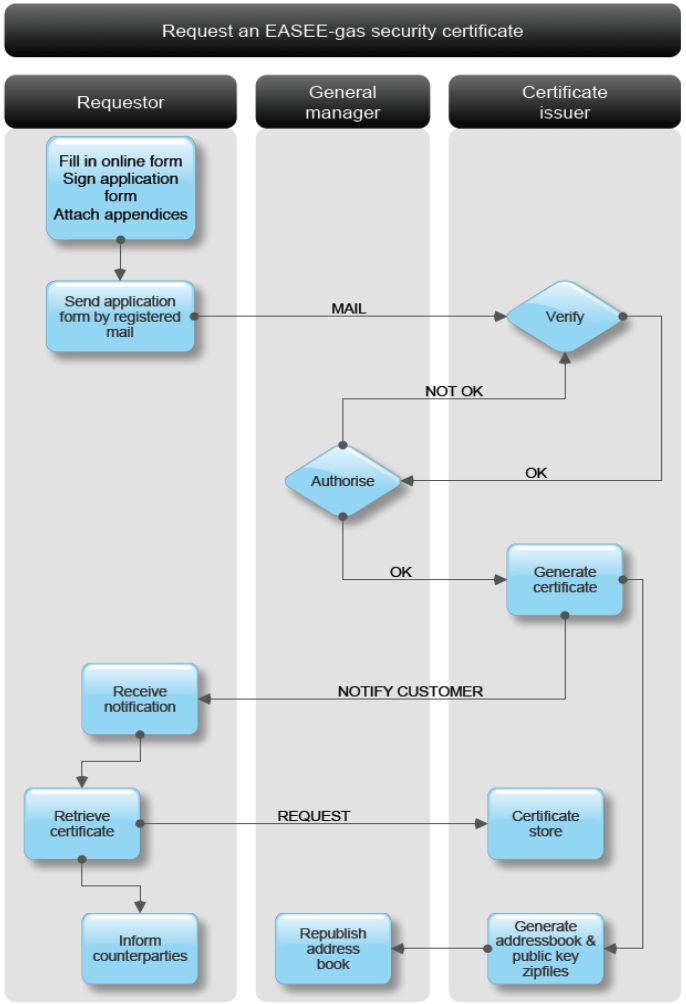
Security

Easier in operations

Procedures

- Trusted Identity Management Description (TIM document)
  - Request new certificate ---------->
  - Renewal
  - Revocation
- Contract with certificate provider

TIM document:

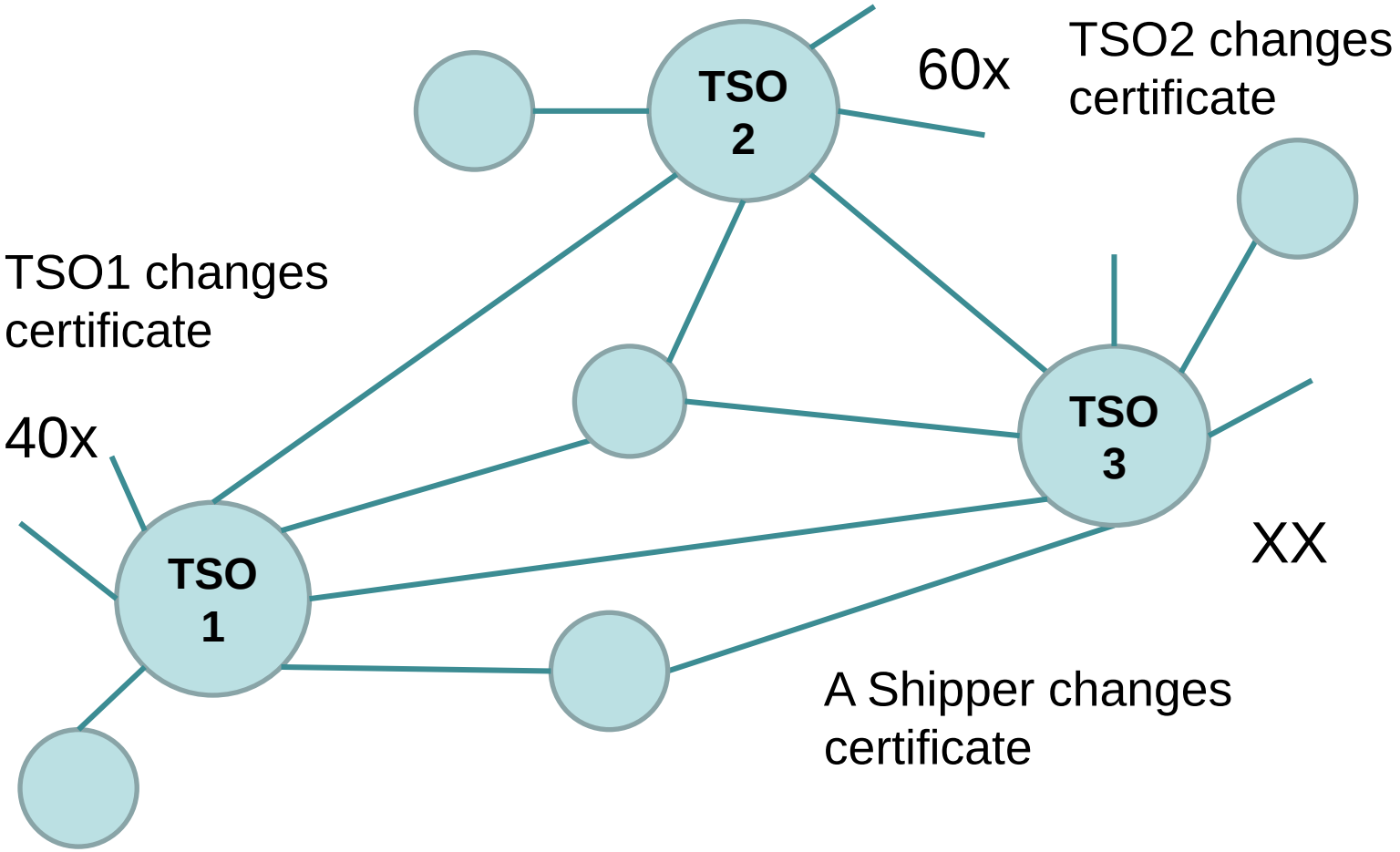


Certificate change process TSO (1)

- Technical aspects
  - Validity period of certificate (=deadline)
  - Most software is not capable of handling different certificates for one party
  - Changes in certificates, e.g. SHA-1 -> SHA-2

- Steps to perform a certificate change, each action e.g. 60x:
  - Inform your counterparties -> contact details, right person?
  - If there are (technical) changes mutual agreement necessary: e.g. trusted 3rd party, hashing algorithm, key length
  - Agree upon a date & time (most processes are time critical)
  - Distribute certificates
  - Perform the actual change
  - Test communication

Certificate change process TSO (2)



A lot of individual actions if certificate change is not coordinated

Lessons Learned

- Procedures are needed.
- Risk? of having one certificate provider
  - However: When DigiNotar failed, in a targeted action the certificate provider was changed and new certificates were generated (risk is not so high)
- No CRL check needed
  - Revocation is a business procedure, not a technical matter
  - Availability for B2B prevails over security
- Use of address book
  - Contacts; technical, administrative
  - Technical data; IP addresses
  - ZIP-file with all public certificates
- Orchestrated certificate change each 3 year (=validity period) is acceptable
  - Certificate project performed by a contracted party (PSvdL)
  - Alternative: frequent bilateral changes in production which cause more work

Conclusions

- Procedures for certificates must be in place
- The fields of the certificate should be standardised
- An explanatory protocol guide is needed
- An address book is very handy
- Controlled issuing of certificates is more secure and increases availability of communication for the TSO's

The conclusions above are easier to realise when:

- One or a few certificate provider(s) are appointed
  - Certificate provider must be able to implement the procedural check

Finnally:

- A technical solution for automatic certificate exchange and implementation would be preferred!

Certificates are necessary, but it is a difficult matter!

Questions?

Three letter acronym free slide

ENTSOG AS4 PoC

Results

Jef De Keyser

Pim van der Eijk

Brussels, 2014-09-09

Agenda -Proof of Concept

1. Why and what
2. Objectives and Participants
3. Test scenario
4. Outcome and results
5. Conclusions
6. Attention points
7. Future activities

1 PoC -Why and what?

Jef De Keyser

PoC - Why and what

> **Why:**

- Demonstrate a functioning AS4 solution
- Validate and fine-tune the AS4 Usage profile
  - detect potential issues in profile definition,
  - check security rules,
  - compatibility and interoperability checks (multiple products)
- Get experts' opinion (Vendors, ENISA, IT people)
- Acquire experience in setting-up/configuring systems

PoC - Why and what

> **What:**

- Set up a test system
- limited number of participants
- Use the AS4 Usage Profile document
- Perform tests according to an agreed scenario

> Provide guidance to all market participants for later AS4 implementation

2 PoC - Objectives and participants

Objectives of Pilot

Objectives:

- Validate (and if needed, fine-tune) the ENTSOG AS4 profile parameters
- Demonstrate interoperable exchange of AS4 messages among multiple organizations using multiple products (or prototypes)
- Validate AS4 functionality

Objectives of Pilot

Out of scope:

- Exhaustively test AS4 conformance and interoperability, including all corner cases
- Certification of solutions
- Security issues e.g. MITM and replay attacks
- testing of functional or non-functional features that are not related to the AS4 protocol
- Other functional tests e.g. message content validation…

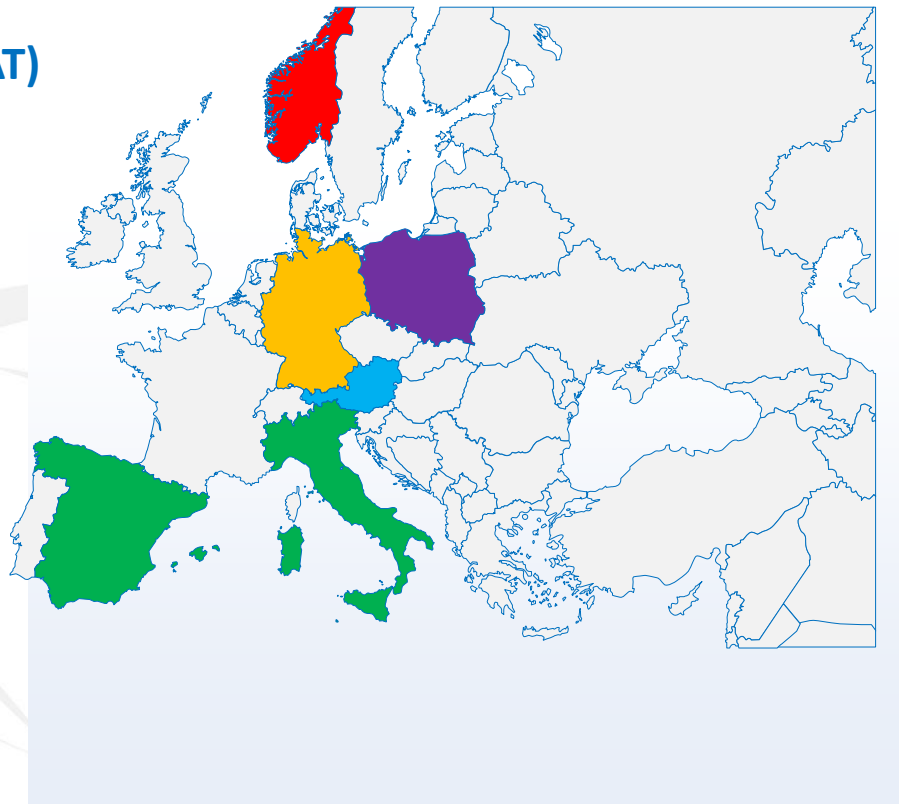
PoC - Participants

> Parties:

- Transmission System Operators:
  - ENAGAS (ES)
  - GAS CONNECT AUSTRIA (AT)
  - GASSCO (N)
  - Gaz-System (PL)
  - SNAM RETE GAS (IT)
  - Thyssengas (Westnetz) (D)
- Trader
  - ENI (IT)

> Solution vendors:

- Ades – AT
- Axway - F
- Seeburger – D
- Software AG – D
- Tibco – USA



3 PoC - Test scenario

PoC - Test scenarios

Core B2B features

>Packaging, metadata

>Compression

Reliable messaging

>Retries, receipts

Security

>Transport layer security

>Message layer signing and encryption

PoC - Test scenario

Test cases	Description	Features
1	TLS Test, Positive Scenario	Transport Layer security (not AS4 related)
2	TLS Test, Negative Scenario	
3	Minimal AS4 Message Exchange	
4	AS4 reliable messaging, basic functionality	Reliable messaging (AS4 features)
5	AS4 reliable messaging, fault scenario	
6	AS4 reliable messaging, retry scenario	
7	AS4 compression feature	Signing Encryption Compression
8	Signing test, positive	
9	Signing test, negative	
10	Encryption test, positive	
11	Encryption test, negative	
12	Signing and Compression	
13	Signing, Encryption and Compression	

4 PoC - Outcome and results

Pim van der Eijk

PoC - Outcome and Results

- **ENAGAS, SNAM and ENI: (Tibco)**
  - No interoperability issues – same product
  - AS4 attribute “Party type” is optional but considered as a required attribute in Tibco (tested with dummy for PoC)
  - TLS 1.2 is not supported:
    - “Unsecure” SSL 3.0 and TLS 1.0 protocols are not rejected
  - Tibco has been informed about detected issues

PoC - Outcome and Results

- **ENAGAS-WESTNETZ/THYSSENGAS: (Tibco-Seeburger)**
  - All scenarios tested
  - Issue with TC13 (order of signing, encrypting and compression)
  - Issue fixed by Seeburger but not re-tested due to lack of time

- **GASSCO-ENI: (Axway - Tibco)**
  - Only positive scenarios tested (late participation of Gassco)
  - Issue found in TC 10 and 13 – encryption. Temporary workaround suggested by Axway.
  - Correction already implemented but not re-tested due to lack of time

PoC - Outcome and Results

>GAZ SYSTEM-WESTNETZ/THYSSENGAS: (Software AG- Seeburger)

- TC1 not tested due to test environment set-up limitation
- TC3 minor issue on specific HTTP 2xx ACK response code to use (request sent to OASIS/Drummond for clarification)
- TC8 WS security timestamp expected in one product, but it is optional in AS4 and in the ENTSOG AS4 Usage profile , will be fixed
- TC10 one product expected receipts for encrypted messages to be encrypted, will be fixed.
- TC13 Technical problem when using separate certificates for signing and encryption in one product.

- Issues reported to vendors, OASIS and Drummond

PoC - Outcome and Results

- **GAS CONNECT AUSTRIA-WESTNETZ/THYSSENGAS: (ADES-Seeburger)**
  - Issues with encryption order and mechanisms used + Java bug
  - All tests completed successfully

- **GAS CONNECT AUSTRIA-SNAM: (ADES-Tibco)**
  - Issues found in TC 11 and 13 – encryption. Analysis still on-going
  - MIME encoding issue

5 PoC – Conclusions

Jef De Keyser

PoC - Conclusions

- The PoC start took more time than planned due to time needed
  - to configure the required test environment and fire-walls,
  - to obtain the required resources and
  - to deploy the products for testing

- The existing AS4 Usage Profile is considered clear to all participants to give guidance for an AS4 configuration

- Most participants were able to run the full test scenario with one or more partners

PoC - Conclusions

- Involvement of multiple products make test more complicated but the successful overall result confirmed the major interoperability of AS4 solutions

- Issues related to security could also appear with other protocols due to the applied increased security standards/requirements

- Thanks to the PoC, issues have been detected at an early stage that have been/are being addressed and will be solved in the future products.

6 PoC - Attention points

PoC – Attention points

When looking for an AS4 solution it might be useful to read the chapter 3 (Proof of concept results) and chapter 4 Summary and conclusions of the ENTSOG AS4 PoC Final Report document.

Although this document is not complete and only a limited number of tests were performed during the PoC, it gives an idea what the potential problems can be when installing a communication system.

Companies should plan sufficient time for implementation

Certificate handling – some standardization and new product features are needed.

Questions

Lunch

13.00--14.00

PoC

Participants view
Future steps

14.00 – 15.30

AS4 POC Snam

Outcomes assessment

Loris Conte

Bruxelles, 09/09/2014

AGENDA

- **AS4 POC Overview and Scope**
- **SNAM Infrastructure**
- **SNAM Infrastructure Customization**
- **Snam/ENI Test Results**
- **Snam/GCA Test Results**
- **Conclusions**
- **Lessons Learnt**

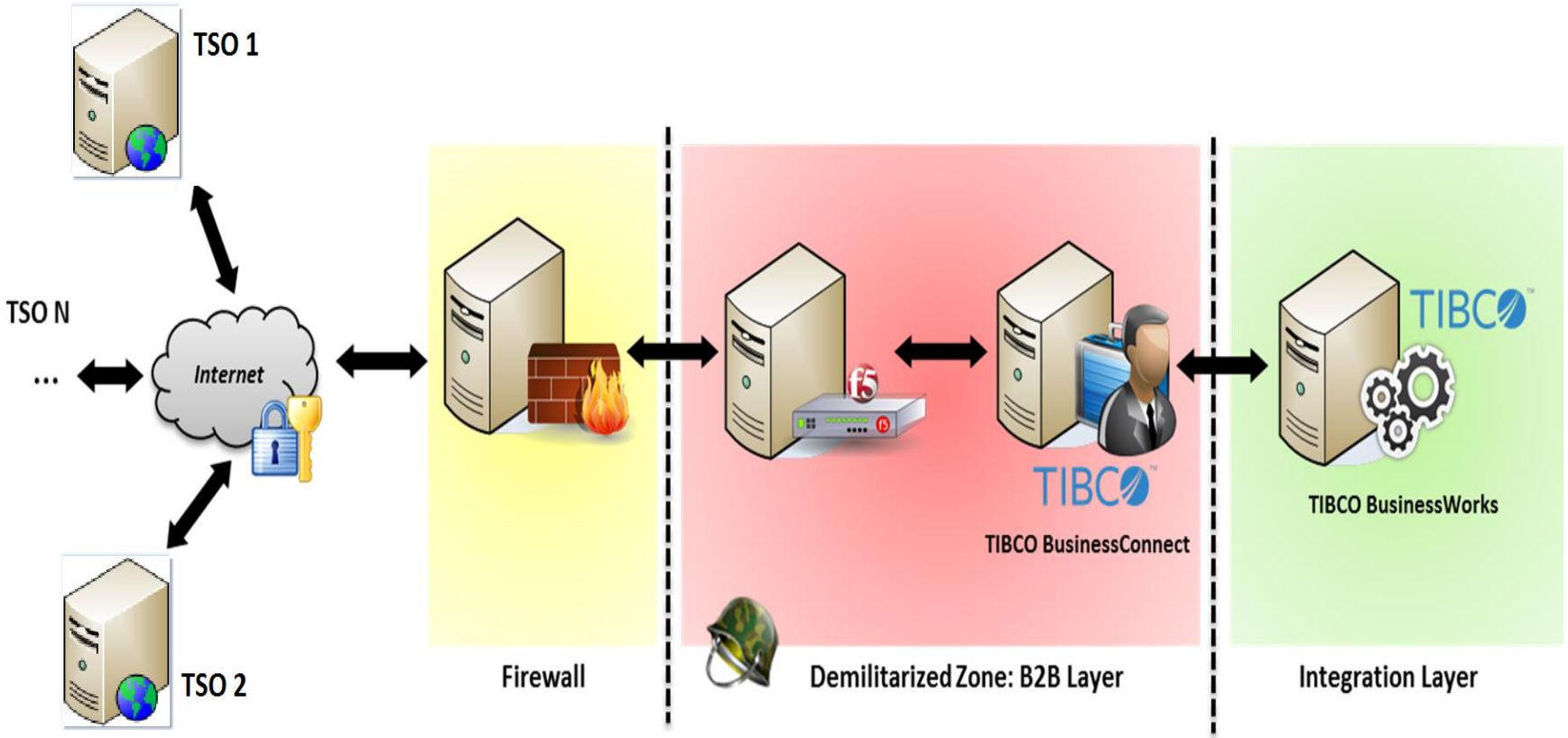
AS4 POC Overview and Scope

Overview (from the official document):

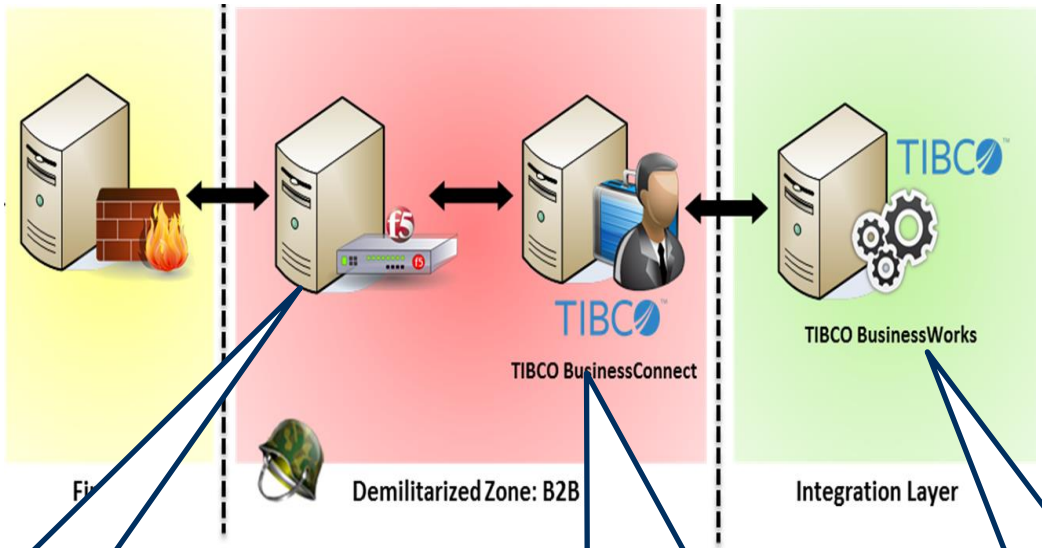
"The network code Interoperability and Data Exchange specifies that for document based data exchanges the AS4 communication standard based on ebMS is to be used as a common protocol."

SNAM participated with the goal of validate and tune the configuration, anticipate issues and build a good know-how for future implementations.

SNAM Infrastructure



SNAM Infrastructure Customization



F5 HW LoadBalancer

- SSL/TLS Encryption enabled.
- Certificates installed.

TIBCO BusinessConnect 6.1.0

- Plug-ins installed:
  - ebMS 3.0
  - ebXML 6.0.1
  - Services plug-in 6.1.0
- TSO profiles configured.
- XSDs installed.

TIBCO BusinessWorks 6.1.0

- New BW processes developed and deployed.

Snam/ENI Test Results

Test results with ENI (Tibco VS.Tibco):

Test	Result
Connection set-up	✓
Partner definition set-up	✓
Minimal AS4 Message Exchange	✓
Minimal AS4 Message Exchange with reliable messaging	✓
AS4 Message exchange with compression	✓
AS4 Message exchange with document signing	✓
AS4 Message exchange with document encryption	✓
Combination of above	

BC

Snam/GCA Test Results

Test results with GCA (Tibco VS. Custom):

Test	Result
Connection set-up	✓
Partner definition set-up	✓
Minimal AS4 Message Exchange	✓
Minimal AS4 Message Exchange with reliable messaging	✓
AS4 Message exchange with compression	✓
AS4 Message exchange with document signing	✓
AS4 Message exchange with document encryption	✗ ✓
Combination of above	

O BC

Conclusions

The solution is overall sound, but some issues were encountered.

- Tibco BC doesn't support:
  - **RSA-OAEP.** RSA 1.5 used as WA.
  - **AES 128 GCM.** AES 128 CBC used as WA.

SR opened by TIBCO: RSA-OAEP supported from Q1-2015.

- X.509 specifications are too tight:
  - Key size of 4096 bit is not supported by the CA used by SNAM (Actalis).
  - Issues with ECDH cipher suite not supported by MS Tools and OpenSSL not so up-to-date.

Engage the CA for new specifications.

Lessons learnt

Be careful on network level/certificate importing activities.

Take some time for partner configuration, before proceeding with tests.

Take a look at field parsing (e.g.: timestamp format) and field position inside the message.

Most important:

Product Change Requests are required in order to fully adhere to the profile.

Q&A

Thank you!

People who worked on this POC:

- **Project managers:** Gianluca Scalmani, Loris Conte.
- **IT architects:** Maurizio Galandrino, Massimo Maiorino, Roberto Palazzo.
- **IT infrastructure:** Ezio Leone, William Dossi.

Energy, everywhere.

Gas Connect Austria GmbH
AS4 Workshop

September 9th, 2014

Ein OMV Unternehmen

GAS CONNECT AUSTRIA

Gas Connect Austria GmbH: Facts and figures

Over 50 years' experience of gas transportation

Operation of Austria's 2,000 km high pressure gas network

Marketing of capacity at 10 cross-border entry/exit points on the Austrian transmission grid

Gas transportation volumes sold entry/exit in 2013: 111 bn cu m

Designation as market area manager (MAM) in 2012

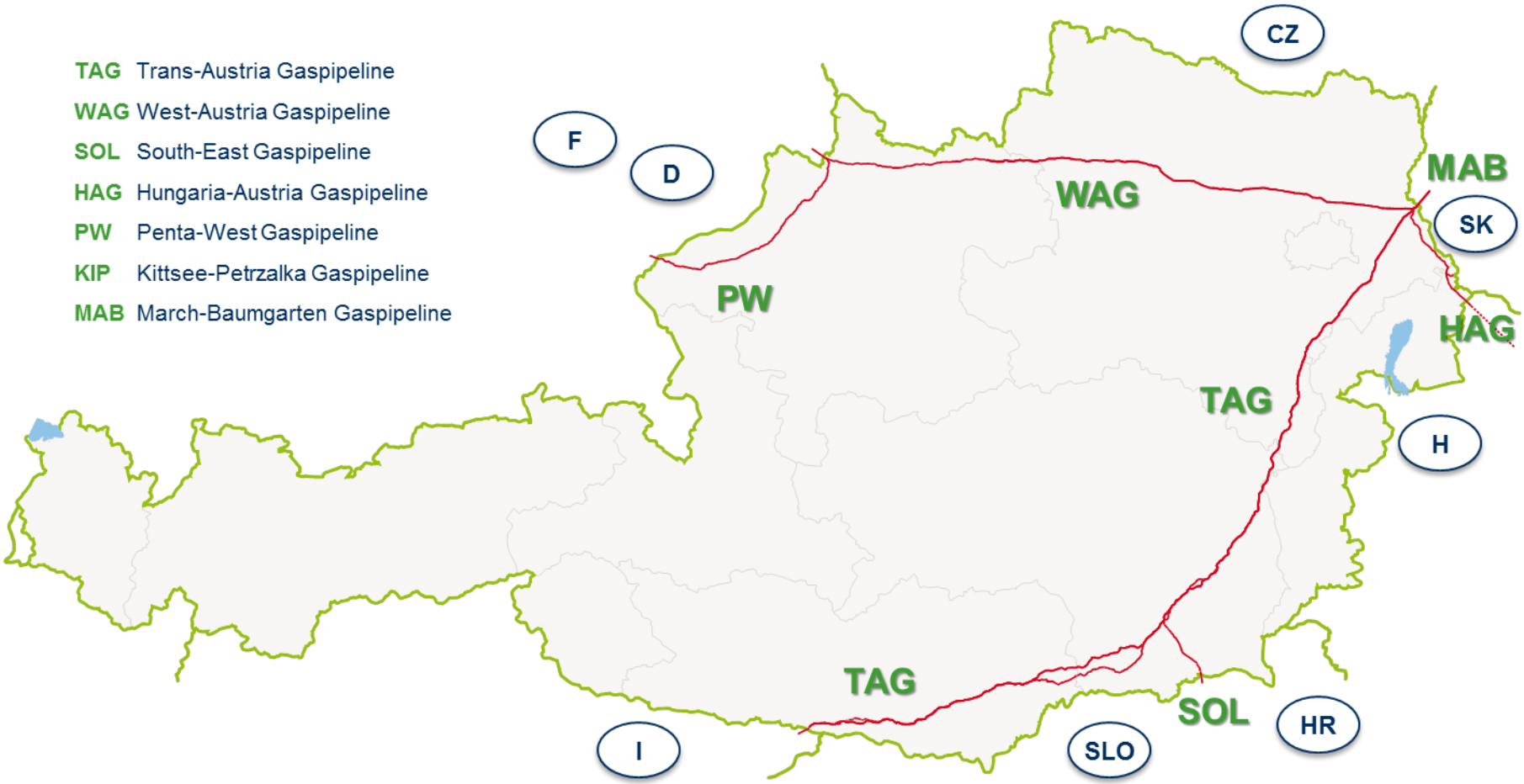
Active membership of European organisations ENTSOG, GIE and GTE

Employees: 400

Wholly owned subsidiary of OMV AG

Headquartered at the floridotower, Floridsdorfer Hauptstrasse, 1210 Vienna

Natural gas grid - transmission



Natural gas in Austria – Baumgarten gas reception station

Key national and European physical hub

Austria's largest reception point and main interconnection station for imports from Russia, Norway and other countries

3 transit systems:
Trans Austria Gasleitung, West-Austria-Gasleitung and Hungaria-Austria-Gasleitung

- 14 compressor units
- 50 employees
- Commissioned in 1958
- First gas shipment from Russia in 1968

Dataformats and protocols

- EDIG@S Version 4.0 xml
- KISS-A (Excel-Format)

- SMTP (E-Mail)
- AS/2
- sFTP

Data Exchange with following partners

- 100-300 messages / day (AS2 / Edig@s)
- Up to 100 messages / day (sFTP / Edig@s)
- Up to 100 messages / day (smtp / KissA)

- 300-500 messages / day (AS2 / Edig@s)
- Up to 100 messages / day (sFTP / Edig@s)
- 500 – 1000 messages / day (smtp / KissA)

Setting up a new communication party (AS2)

- Information exchange on business level
  - Network parameters: IP addresses, ports
  - Application parameters: protocol, IDs, certificates, parameters
- Network tests
  - Testing the connection, firewall settings
- Application tests
  - Testing the protocols (acceptance, productive system)
- Content tests
  - Formats (Edig@s), content (parameters, values)

ADES - Corporation

- ADES Echtzeitdatenverarbeitungssysteme GmbH Vienna, www.ades.at
  CEO: Leopold Wagner

- Christoph Holper c.holper@ades.at
  Software engineering (communication standards, protocol implementations, customer applications, automation integration)

- Software-company specialized in software-engineering and customer-support.

- Products and services for companies in energy, industrial, automation, environment and information-technology.

- ADES is software-provider for Gasconnect Austria and many other major companies in Austria and Europe

ADES – AS4 implementation

- One single Linux server (File Processing Appliance) hosting every communication-specific application (FTP/SFTP, IEC 60870, AS2, AS4, ...)

- Interfaces to enterprise backend-systems, status- and workflow-visualization, archive-presentation, ... and customer-specific modules

- Packaging basic technology (MIME, XML, SOAP, X.509, Base64, ...) to required functionality (XML-SIG, XML-ENC, ebXML, ...) instead of customizing unmanaged frameworks

Proof of Concept – Results / Questions

Successfully tested with 2 parties within the PoC.
From our perspective further information about the following issues can be helpful or are less defined.

– Content-specific

- Party-description: Impact of Party-Role to further processing in AS4 and backend-systems

- Configuration-identification: Find proper configuration for the remote party (IP, IDs, P-Mode, agreement, combination, ...)

Proof of Concept – Results / Questions

– Implementation-specific

- Reject/Failure: HTTP (202 vs. 204), SOAP (1.1 vs. 1.2), AS4

- Encryption: Different encryption-specific parameters (initialization-vector, padding)

- Canonicalization: Impact of MIME-ContentType and PartInfo-MimeType to canonicalization and support of XML-canonicalization

- X.509-token: Normalization of issuer-string (LDAP DN)

Thank you for your attention

ENTSOG‘s PoC
and
AS4‘s future role in Germany

Zoran Petrovic
z.petrovic@seeburger.de

Overview

- About the Parties Involved
- (Selected) Results from the PoC
- What about AS4 in Germany?

About the Parties Involved

Westnetz

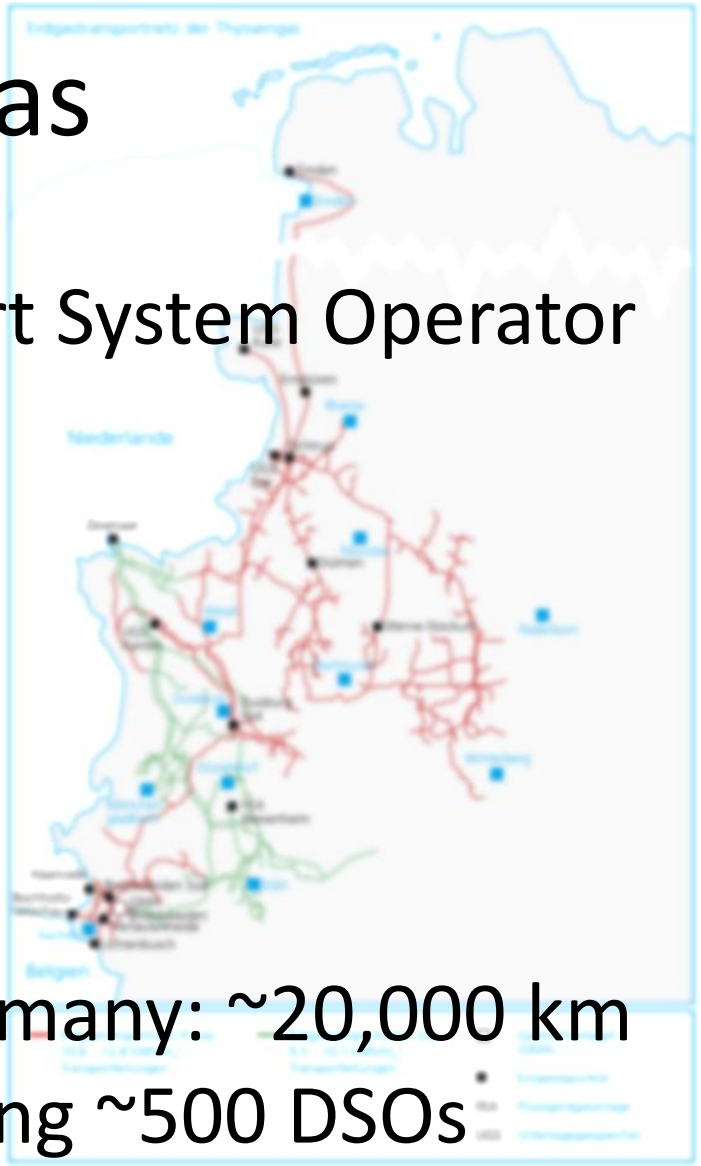
A Distribution System Operator in western Germany.

Turnover: 5.6 bn EUR
Employees: 5,200

195,000 km network length (electricity)
26,000 km network length (gas)

Thyssengas

An independent Gas Transport System Operator in western Germany.



Network length: 4,200 km
Employees: 290

Takes part in NetConnect Germany: ~20,000 km high-pressure pipelines, serving ~500 DSOs

SEEBURGER

A privately-owned, independent business integration software company.

Customers: > 9,000

Employees: 600

Over 250 customers in the energy industry: Westnetz, RWE, E.ON, EnBW, LichtBlick, ..

(Selected) Results from the PoC

Our Setup

Problems:

- Setting up System Landscape/Firewall in time
- Keeping daily work uninterrupted
- Ensuring easy access for developers

Solution:

- Keeping PoC systems entirely separate from productive systems

The tests (1/2)

Enagás (Spain)	Tibco
Scenario 13 – order signing, encryption & compression	

GAS CONNECT AUSTRIA	ADES
Non-Java based system (Apache). • Java core bug: Not all primes accepted • WSS4J: AES128-gcm interop issue	

The tests (2/2)

Gaz-System (Poland)	Software AG
Scenario 3: Different interpretation of 2xx HTTP response code (OASIS vs. Drummond) Scenario 8: WS-Security Timestamp expected for duplicate detection	

Lessons Learned

- Interoperability higher than expected
- Connection parameters easy to exchange
- System landscape can be a sticking point
  - Adapter Rollout
  - Certificate Exchange
  - Firewall
- Encryption still ain‘t easy. Sometimes, a bug is deep down.

What about AS4 in Germany?

M2M Communications today

- Over 900 network operators (electricity), over 1,000 suppliers
- EDIFACT based communications
- Bi-annual releases (EDI@Energy)
- Transport via
  - Email (S/MIME, hopefully)
  - AS2

Challenges with Mail/AS2

- Many market participants are small(ish)
- MDN? Encryption?
- Certificate Management
- Configuration
  - Firewall
  - Protocol details and extra setups for individual market partners
- Smart Metering looming ahead

A fresh start with AS4..

- AS2‘s spiritual successor
- Sound, modern protocol
  - WebServices
  - Content agnostic
  - MDN, encryption, compression, non-repudiation
  - Ready for a better Certificate Management
- Good standards governance (as seen with OASIS and ENTSOG)

Thanks for joining us today.

**Progress lies not in enhancing what is,
but in advancing toward what will be.**

Khalil Gibran

Questions?

(SEEBURGER‘s AS4 system is available now.)

7 Future activities

Jef De Keyser

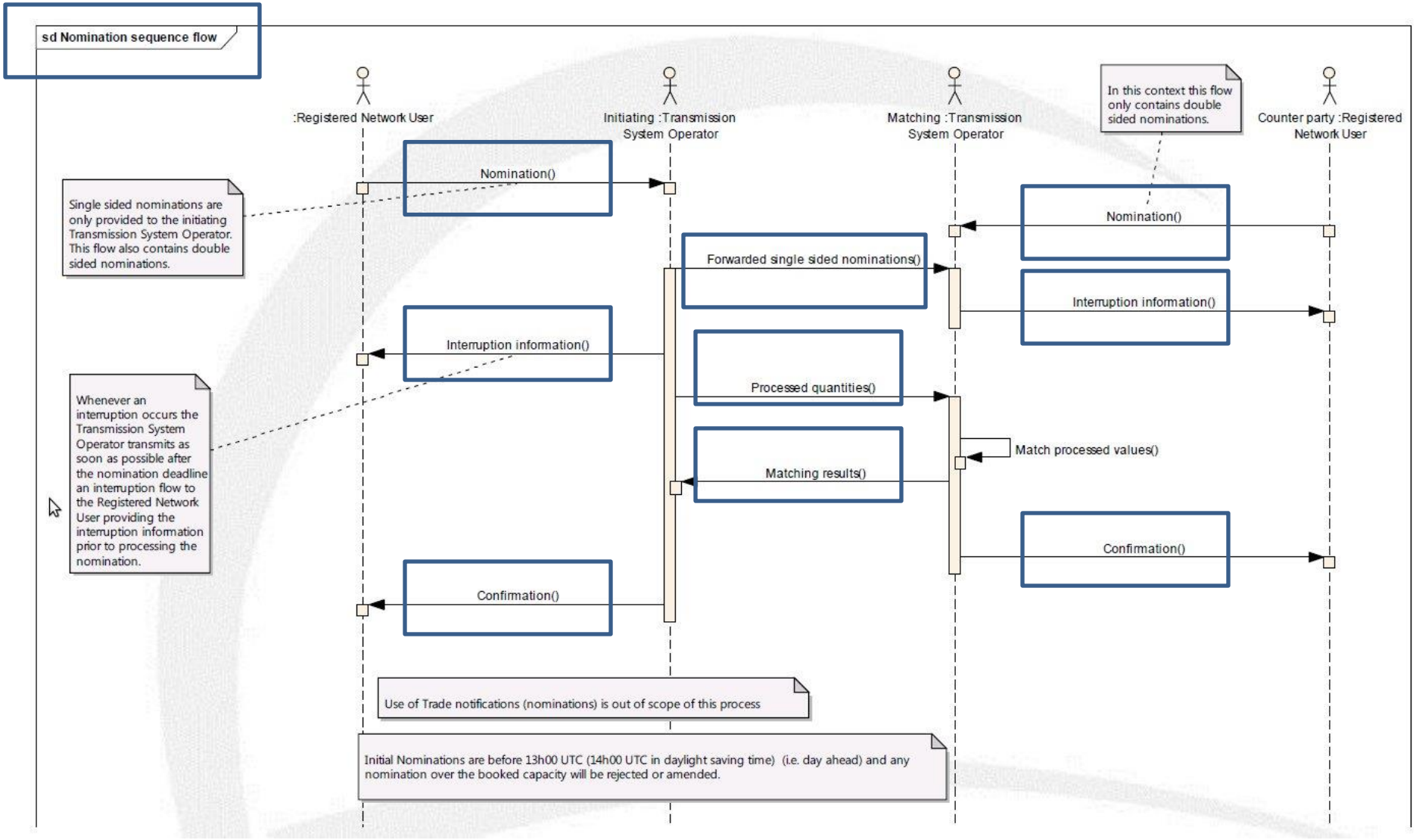
AS4 – Future activities

- ENTSOG will keep the AS4 Usage Profile document up-to-date and publish it on its website

  - E.g. define **Service** and **Action** header elements for business processes
  - Define recommendations/rules for **ConversationID**, **MessageID**…
  - Give more guidance when implementation questions pop-up

Nomination Service

Nomination Actions



```
<S12:Header>
    <eb3:Messaging wsu:Id="_18f85fc2-a956-431e-a80e-09a10364871b">
        <eb3:UserMessage>
            <eb3:MessageInfo>
                <eb3:Timestamp>2014-04-03T14:49:28.886Z</eb3:Timestamp>
                <eb3:MessageId>2014-921@5209999001264.example.com</eb3:MessageId>
            </eb3:MessageInfo>
            <eb3:PartyInfo>
                <eb3:From>
                    <eb3:PartyId>21X-EU-A-X0A0Y-Z</eb3:PartyId>
                    <eb3:Role>TransmissionSystemOperator</eb3:Role>
                </eb3:From>
                <eb3:To>
                    <eb3:PartyId>21X-EU-B-P0Q0R-S</eb3:PartyId>
                    <eb3:Role>MatchingSystemOperator</eb3:Role>
                </eb3:To>
            </eb3:PartyInfo>
            <eb3:CollaborationInfo>
                <eb3:Service>http://entsog.eu/nomination/1.0</eb3:Service>
                <eb3:Action>ForwardNomination</eb3:Action>
                <eb3:ConversationId>2014-921</eb3:ConversationId>
            </eb3:CollaborationInfo>
            <eb3:PayloadInfo>
                <eb3:PartInfo href="cid:e1d-8821-49191b4ece93@sender.example.com">
                    <eb3:PartProperties>
                        <eb3:Property name="MimeType">application/xml</eb3:Property>
                        <eb3:Property name="CharacterSet">utf-8</eb3:Property>
                        <eb3:Property name="CompressionType">application/gzip</eb3:Property>
                    </eb3:PartProperties>
                </eb3:PartInfo>
            </eb3:PayloadInfo>
        </eb3:UserMessage>
```

AS4 – Future activities

> **Certificate management** (for digital signatures and encryption):

- Certificates have a limited lifetime (validity period typically 3-5 year)
- Renewal requires
  - manual intervention of IT security people
  - all your counterparties have to update at the same time
  - increased complexity when the number of partners grows
  - increased risk for failures and system unavailability
- Important coordination work required

AS4 – Future activities

- ENTSOG intends to work with stakeholders to study possibilities to manage and handle the replacement of user certificates automatically

  - Automated Certificate Exchange:
    - Owner of a certificate can change its certificate at any time and send it to its partners
    - Certificate updates are processed automatically (if the AS4 product has this feature)
    - No interruption, new certificates are phased-in via an automated process
    - Concept defined in IETF CEM (Certificate Exchange Messaging)
    - Could be generalized to more general configuration exchange mechanism
    - **Vendors** should be involved and support this functionality in their products

AS4 – Future activities

- Expected publication INT NC April 2015

- ENTSOG will support its members through the phase of implementation of INT NC (April 2015 – April 2016):

  - create the FAQ
  - provide expertise and share experience gained through PoC
  - organize internal meetings

If required additional support for TSOs can be considered

Questions