

# nominet

## Technical Workshop

Jay Daley

A decorative graphic on the right side of the slide, consisting of numerous thin, white, wavy lines that create a sense of motion and depth against the solid purple background.

Technical Workshop  
Agenda

nominet

Data Restructuring & Major Systems Upgrade

Extensible Provisioning Protocol

DNSSEC

Centre of Technical Excellence



Technical Workshop

# Data restructure & Major Systems Upgrade



## The initial diagnosis

---

- Customer data was not joined up
  - No integrated billing
  - Worst example was domain names
  - Full copy of the registrant data for each domain
  - Actions across multiple domains were complex
  - Lots of people got lots of letters
- Multiple online systems designed in different ways
  - Different authorisation for different systems
  - Completely different look and feel
  - Same issues for systems staff used
- Adding functionality is difficult and time consuming
  - Registrars need web based interface and EPP
  - Paper processes need to move online

## Deeper problems

---

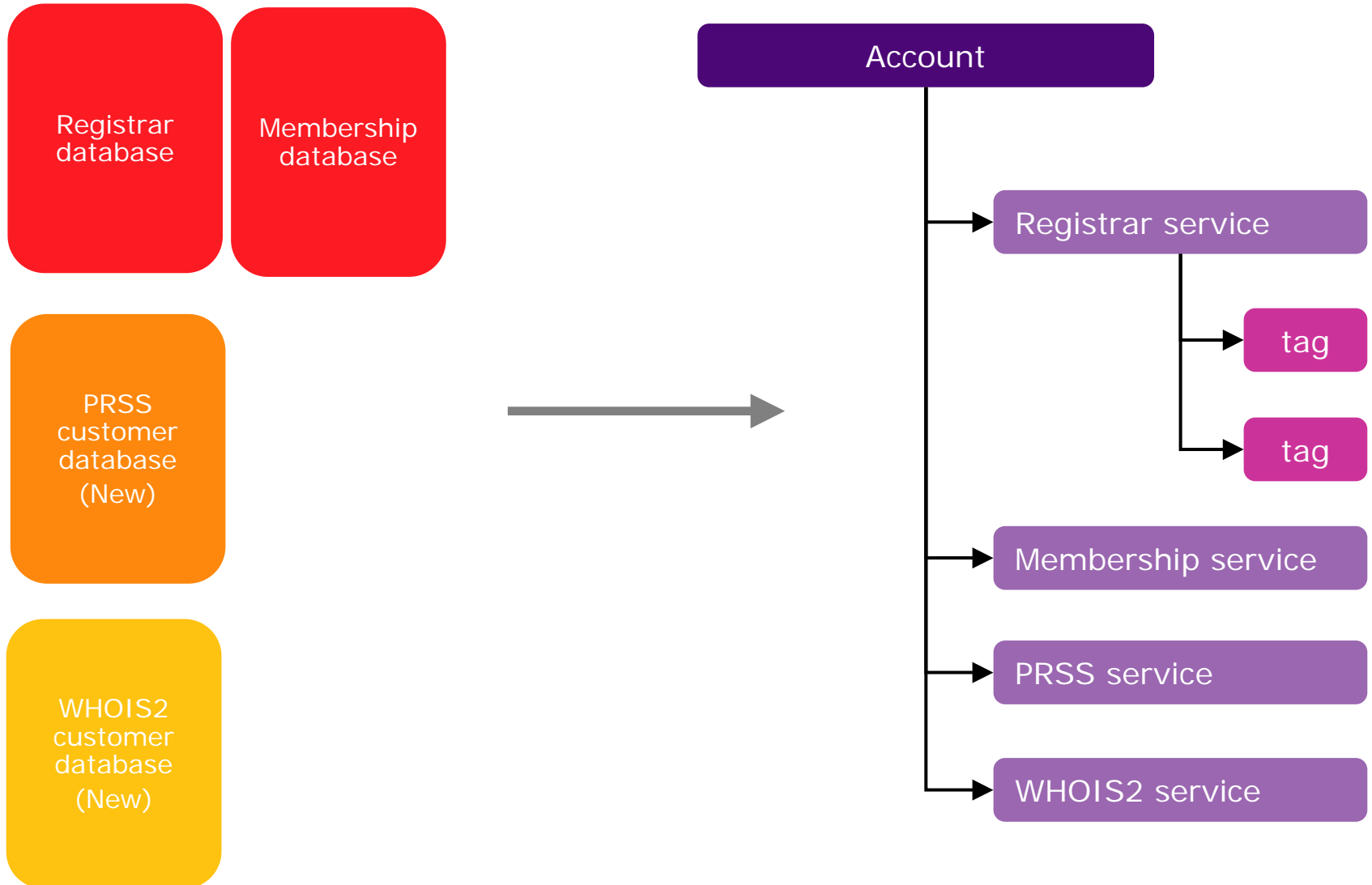
- Piecemeal technical architecture
  - Organic growth, no strategy
  - Difficult and time-consuming to change
  - Would not scale
- Fallen behind on modern functionality
  - Couldn't support drive to modernise processes
  - Couldn't support more sophisticated interaction
    - E.g. surveys, secure messages
- Disjoint user experience
  - Low usability
  - Accessibility hit and miss

## The work plan

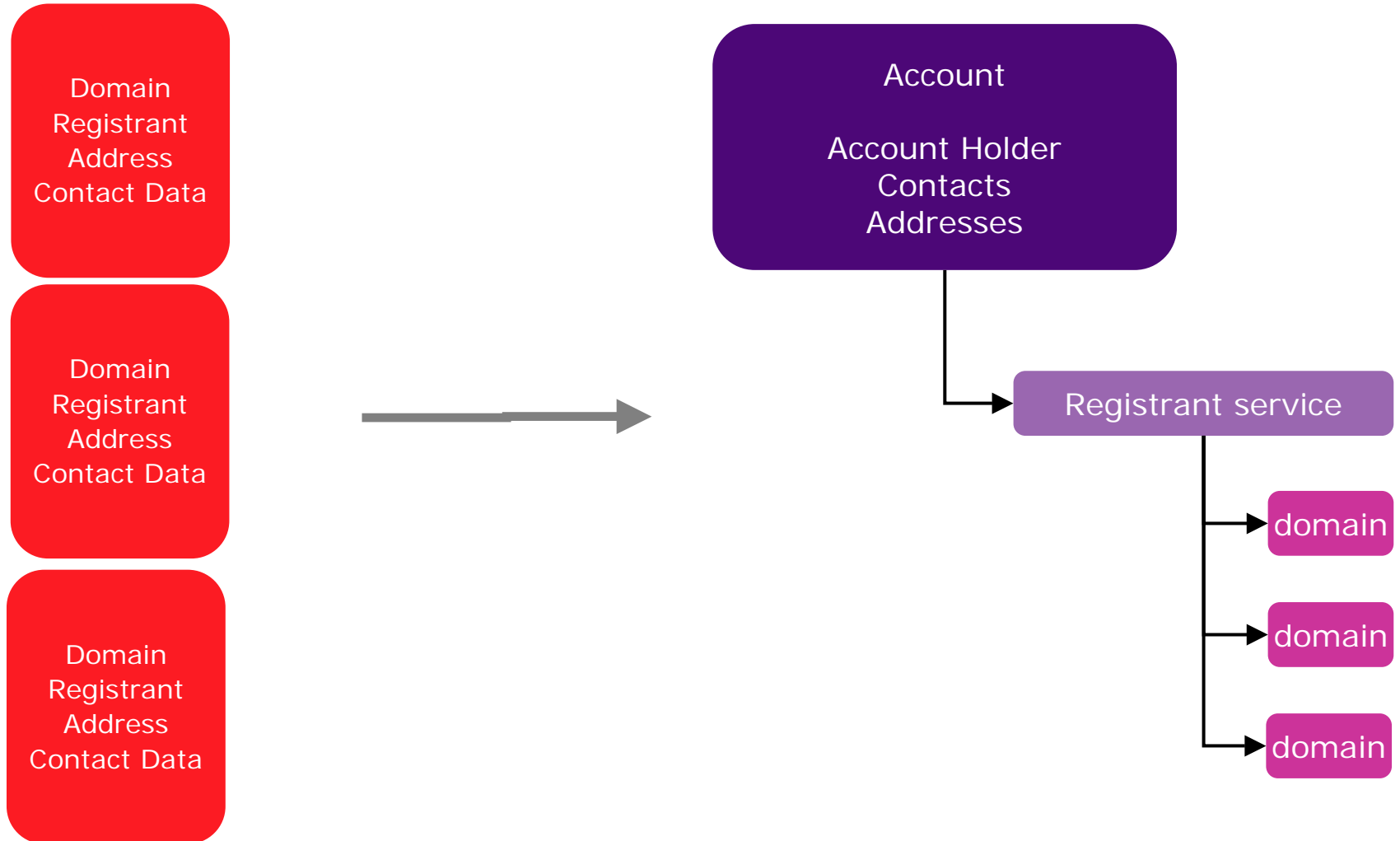
---

- Introduce an account based data structure
  - Buy a service and get an account
  - New services added to the same account
  - One set of data per account
- Single online application for managing your account
  - Single login for all services
  - More services means more tabs become visible
  - Used by all customers - registrars, registrants, PRSS users, etc
- Single internal application for staff
- Loads of new functionality

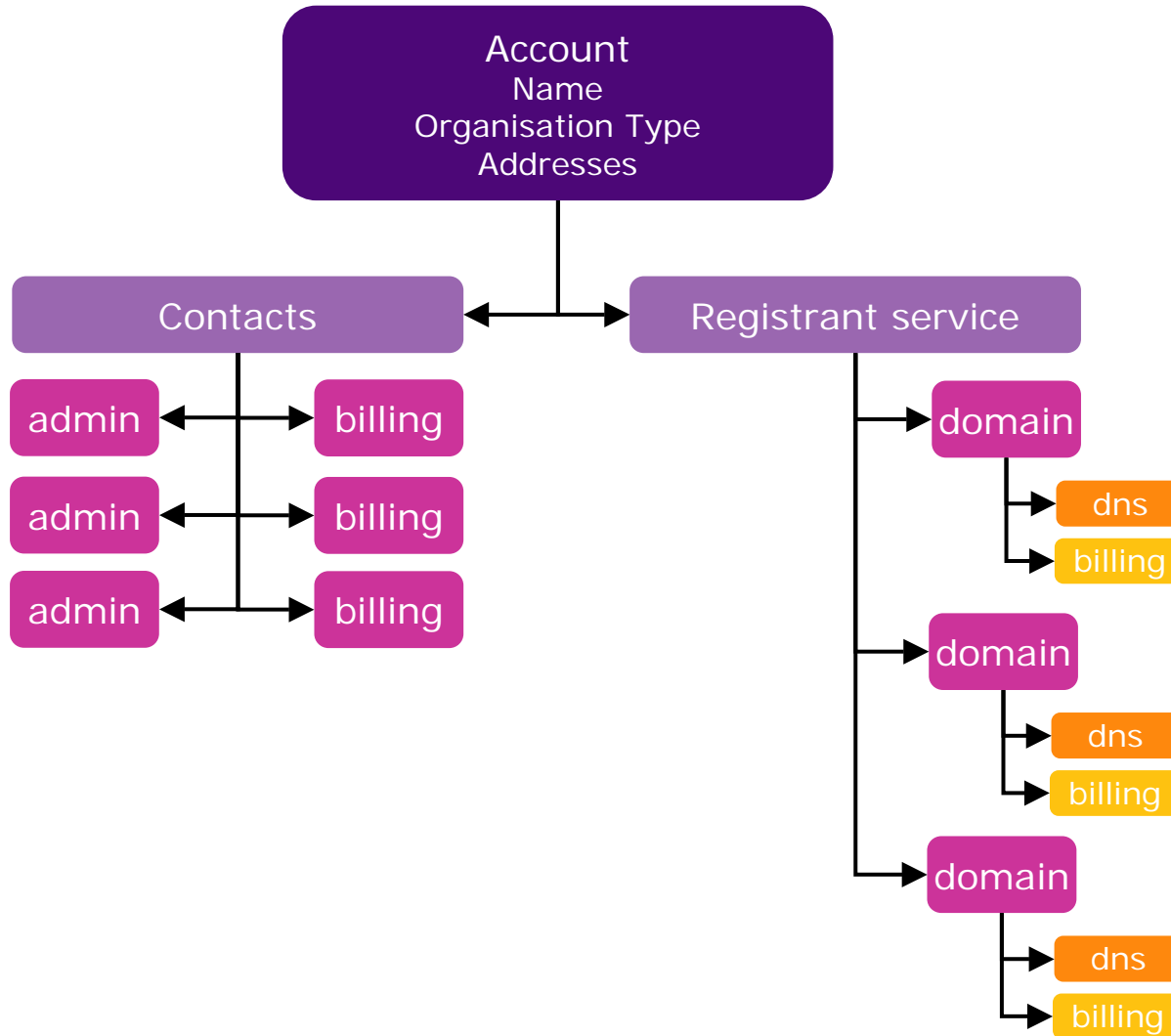
# Account based structure



# Account based structure



# Account based structure



## The high level outcomes

---

- A flexible and modern architecture
  - Small set of technologies
  - Easy to add new features
  - Easy to change, release and manage
  - Scale gracefully
- Support modernisation of processes
  - Automation of paper based systems
  - New interactions
- Consistent, high-quality user interface
  - Focus on usability, security and accessibility

# Every system needed to be rewritten

---

- Registrants online - registrants correct their details
  - Unique web front end
  - Password letter send to enable authorisation
  - Internal Java client
- Tag change - registrants change tag for a domain
  - Unique web front end
  - No password, used data matching and signature
  - Internal web client
- Automaton
  - Critical high volume system
  - Internal C++ client for staff
- Billing system
  - Domain renewals and cancellations
  - Internal Oracle Forms client for staff
- Member/Registrar management system
  - Linked to Automaton management
  - Internal Oracle Forms client for staff

## New systems needed to be added

---

- Single login module
  - With welcome emails not letters
- PRSS management system
  - Used to be paper file and uploaded of users
- WHOIS2/DAC management system
  - Registrars control their access
  - Internal management for staff
- Mailing list subscriptions
  - Link to member/registrar database
- Secure messaging
- Registrar data management
  - Change address/contact details
  - Full access to financial information
  - Manage PGP keys online
- New Internal client to support all of this

## The implementation

---

- Released in stages
  - Stage 1, 2005
    - Account structure introduced.
    - Member and registrar basic data manipulation.
  - Stage 2, 2006
    - Enhanced functionality for registrars
  - Stage 3, 2007
    - Domain names and registrant data normalised
    - Existing registrant services automated
  - Stage 4, 2008
    - Web based domain management for registrars
    - Further registrant processes automated (transfer)
    - New DRS
    - Multi-year registrations

## Stage 3 had some issues

---

- Backwards compatibility less than expected
  - Registrars could not ignore this change
  - Some things worked too differently
- Documentation quality highlighted
  - Major rewrite needed after launch
  - Still a long way from the best of class
- Testing facilities inadequate
  - Registrars had to learn the hard way
- Bugs at the launch
  - Our testing was inadequate
  - Some services suffered
- Greatly underestimated scale of the work
  - Took much longer than advertised

## Moving on

---

- Most registrars still using 'old' data structure
  - New structure will make life easier
- Reminder - New data structure
  - Extended Automaton command set
  - Four objects can now be manipulated
    - Accounts
    - Domains
    - Nameservers
    - Contacts
- EPP now in beta
  - Better documentation following lessons learned
  - Full test infrastructure
- Final phase in development

## And for the geeks

---

- Front end
  - Solaris servers (V240s) running Apache
  - Load balanced (LLB) on small HP servers
  - Stateless - horizontal scaling
- Middleware (1)
  - Java beans in servlet container (Tomcat) with Spring as IOC layer.
  - Mix of Hibernate and custom persistence layer (Catnap)
  - Use Hessian for IPC
- Middleware (2)
  - All C/C++
  - Automaton functionality only
- Database
  - Oracle 10g cluster
  - Lots of PL/SQL

## Some questions

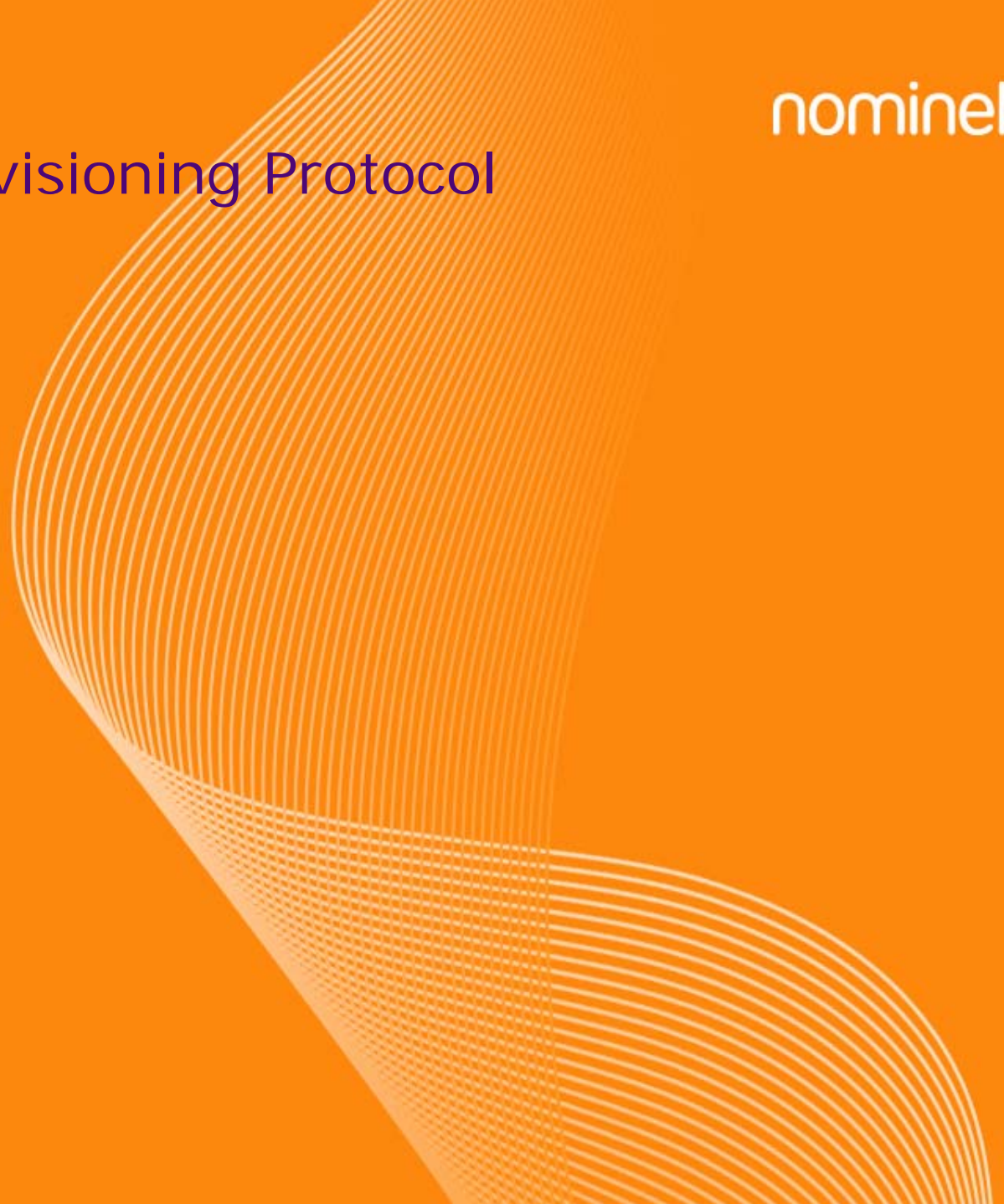
---

- What more could we learn from this process?
- What more do we need to do to get you to use the new data structure?

Technical Workshop

# Extensible Provisioning Protocol

nominet



## What is EPP?

---

- A way for registrars to talk to a registry
  - International standard - widely supported
  - XML based
  - Generally real time (synchronous)
  - Extensible to support local data structures
  - Supports persistent connections
- But ...
  - EPP is another way of accessing the registry
  - Not replacing Automaton - supplement it
  - And web-based access to come (see our stand)

## Some example EPP

---

**<info>**

Returns  
information on a  
domain.

**Automaton  
equivalent**

Query

### Example code

```
<epp>
  <command>
    <info>
      <domain:info
        xmlns:domain="http://.../nom-domain-1.0"
        xsi:schemaLocation="http://.../xml/nom-domain-1.0
          nom-domain-1.0.xsd">

        <domain:name>example.co.uk</domain:name>

      </domain:info>
    </info>
    <ciTRID>ABC-12345</ciTRID>
  </command>
</epp>
```

1. Open an SSL connection
2. Login
3. Send a command
  - create, renew, update, delete, info, transfer
4. Wait for a response
  - Or send another command (asynch)
5. Poll for any notification
6. Keep going until you are finished
  - Repeat steps 3, 4 or 5
7. Logout
8. We will limit connections similar to DAC or WHOIS2

## Schemas

---

- Formal definition of legal EPP syntax
- Some basic ones in the standard
  - epp-1.0.xsd and eppcom-1.0.xsd
- Our extensions
  - nom-domain-1.0.xsd
  - nom-account-1.0.xsd
  - nom-contact-1.0.xsd
  - nom-ns-1.0.xsd
  - nom-notifications-1.0.xsd
- Your code must validate against these schemas

## How our EPP is different

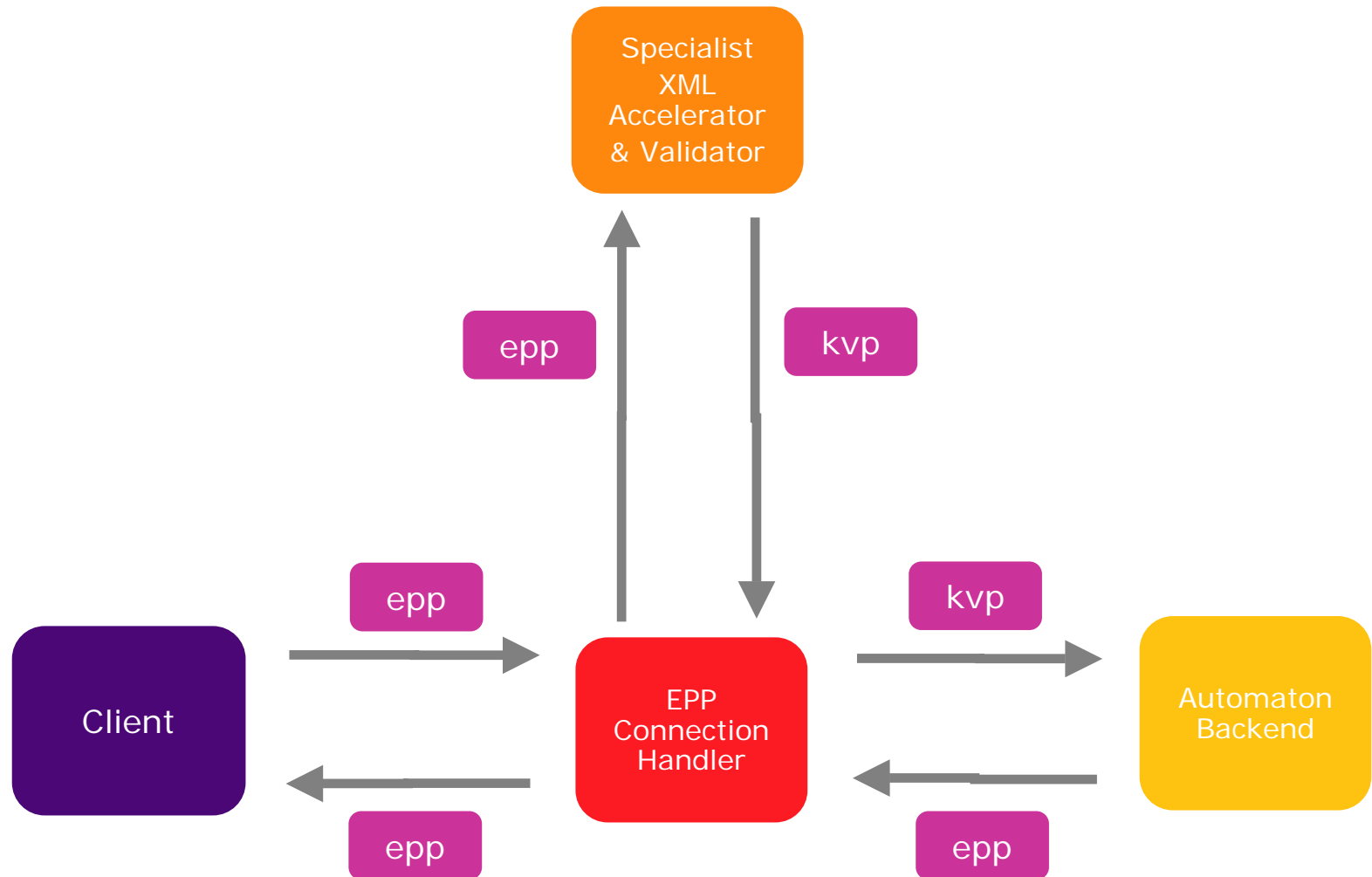
---

- Don't forget - EPP is intended to be Extensible
  - Does not fit our data structure, so have to extend
  - Designed for gTLDs (.com etc) with very different data structure
  - Minimal input from ccTLDS (our fault)
- Accounts - new schema
- Notifications - new schema
- Host - don't use, use ns instead
- Contacts - our variant
- Domains - our variant

# Extensible Provisioning Protocol

## EPP under the hood

nominet



## Next steps with EPP

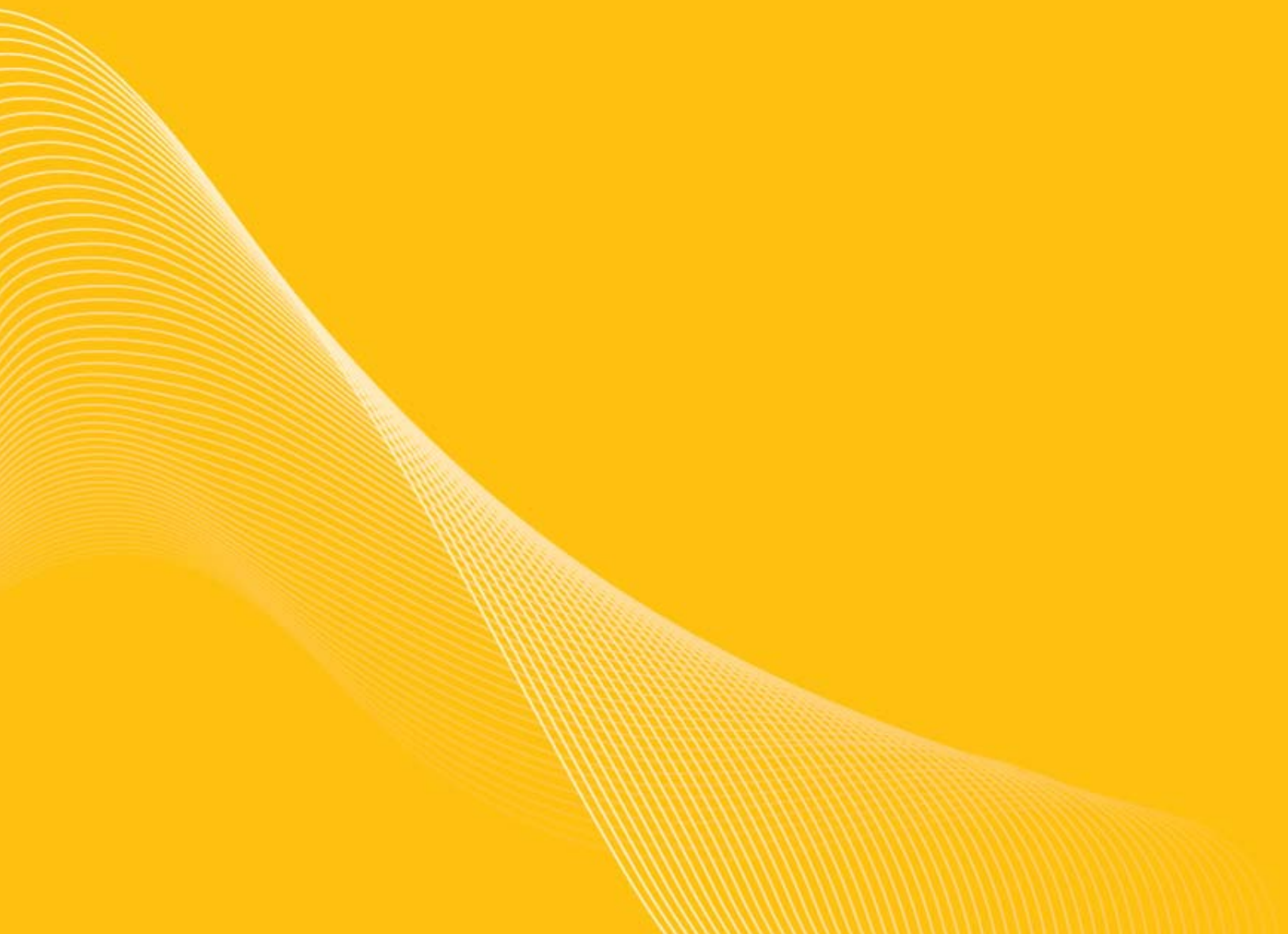
---

- Notifications to be released
  - Tag change notifications and handshake
  - Manually processed referrals (e.g. ltd.uk domains)
  - Data change by registrant
  - Poor quality data
  - Cancellation notifications
- Define and publish access limits
- Feedback sought
- Go live



Technical Workshop  
DNSSEC

nominet



## The need for DNSSEC

---

- Real security issue
  - DNS responses can be spoofed
    - You send query, attacker sends forged reply
  - Your PC misdirected for one or all sites
  - Now being used as targeted attacks
- Solution
  - Signatures are added to DNS responses
  - Establishes authenticity and integrity of data
  - Queries are not secured at all
  - Different keys at each level of the DNS

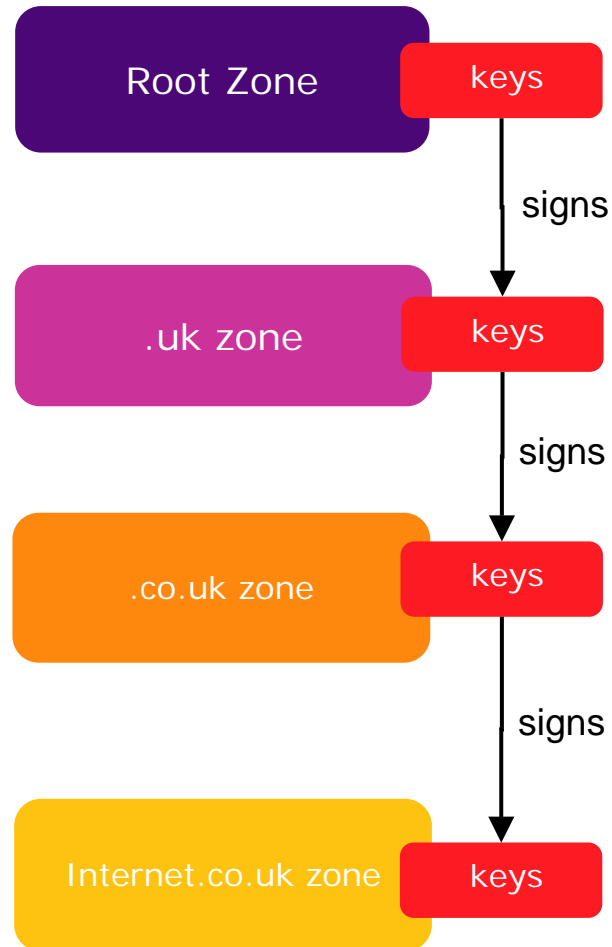
## Why DNSSEC should interest you

---

- Building a secure Internet
  - Top concern of Internet users
  - Major issue in IGF and for politicians
- DNSSEC is a key building block
  - Each layer secured in turn
  - DNS is fundamental layer
  - Some technologies directly rely on it
    - DKIM - preventing spoofed email
- It is actually quite easy
  - Don't believe the hype
  - Using protocol different from understanding details

# Chain of trust

---



## Quick overview of the protocol

---

- Records for authoritative data are signed
  - e.g. www, MX records, A records
- Delegations are different
  - Nameserver records not signed
  - New DS records with key ID for delegation are signed
- Two types of keys
  - Key Signing Keys (KSK) - sign other keys
  - Zone Signing Keys (ZSK) - sign data
  - Public key cryptography
- So for co.uk
  - You give us IDs of KSKs
  - We sign them and publish DS records
  - You publish KSKs and ZSKs in your zones in DNSKEY records



# A DS record

---

```
dskey.example.com. 86400 IN DS 60485 5 2 ( D4B7D520E7BB5F0F67674A0C  
CEB1E3E0614B93C4F9E99B83  
83F6A1E4469DA50A )
```

-- generated from the following DNSKEY record --

```
dskey.example.com. 86400 IN DNSKEY 256 3 5 ( AQOeiiR0GOMYkDshWoSKz9Xz  
fwJr1AYtsmx3TGkJaNXVbfi/  
2pHm822aJ5iI9BMzNXxeYcmZ  
DRD99WYwYqUSdjMmmAphXdvx  
egXd/M5+X7OrzKBaMbCVdFLU  
Uh6DhweJBjEVv5f2wwjM9Xzc  
nOf+EPbtG9DMBmADjFDc2w/r  
ljwvFw==  
); key id = 60485
```

## Our involvement

---

- Preventing zone file enumeration
  - Uses artefact of original DNSSEC to allow enumeration
  - Designed new mechanism to fix this
  - Pushed through IETF and supported development
- Enabling gradual introduction
  - Original DNSSEC meant all or nothing
  - Huge increase in resources immediately
  - New mechanism allows introduction piecemeal
  - As a sub zone is signed, so the parent secures it
- Worldwide experts
  - Leading author of standards works for us
  - Taken lead on policy over signing the root

# Implementing DNSSEC

---

- What needs to happen to kick start it?
  - Need the root signed
    - Can actually implement now, but only as an island
    - Live issue with real impetus
  - Need registries to support it - we are working hard
  - Need final standards signed off - any day now
- Next steps for you
  - Check your DNS servers are up to date and support DNSSEC
  - Once root is signed - configure root keys into your servers
    - Same way you configure root server addresses
  - Receive keys from end users or create yourselves
  - Upload key IDs to us using Automaton/EPP
  - May need bigger boxes (millions of RRs)
- Away we go

Technical Workshop

Centre of Technical Excellence

nominet



## A strategy in steps

---

- Spotting important technologies in the early phases
  - Central Numbering Database
  - Emergency Location Services
  - Automated abuse detection
  - Name Server Control Protocol
- Participating in international design groups
- Educator
  - Blog articles (<http://blog.nominet.org.uk/tech>)
  - Presentations
- Early developer
  - Testbeds for customers - DNSSEC
  - Example code - dnscruby
- Innovator
  - Link with Academia and other partners - KTP with Brookes

## Finish UP

---

- Data restructuring
  - What we've done, why it took so long, what comes next
- EPP
  - How it works, how we are different, what you need to do
- DNSSEC
  - The next big thing
- Centre of Technical Excellence
  - Our strategy for becoming leading edge and staying there
  
- Any questions?