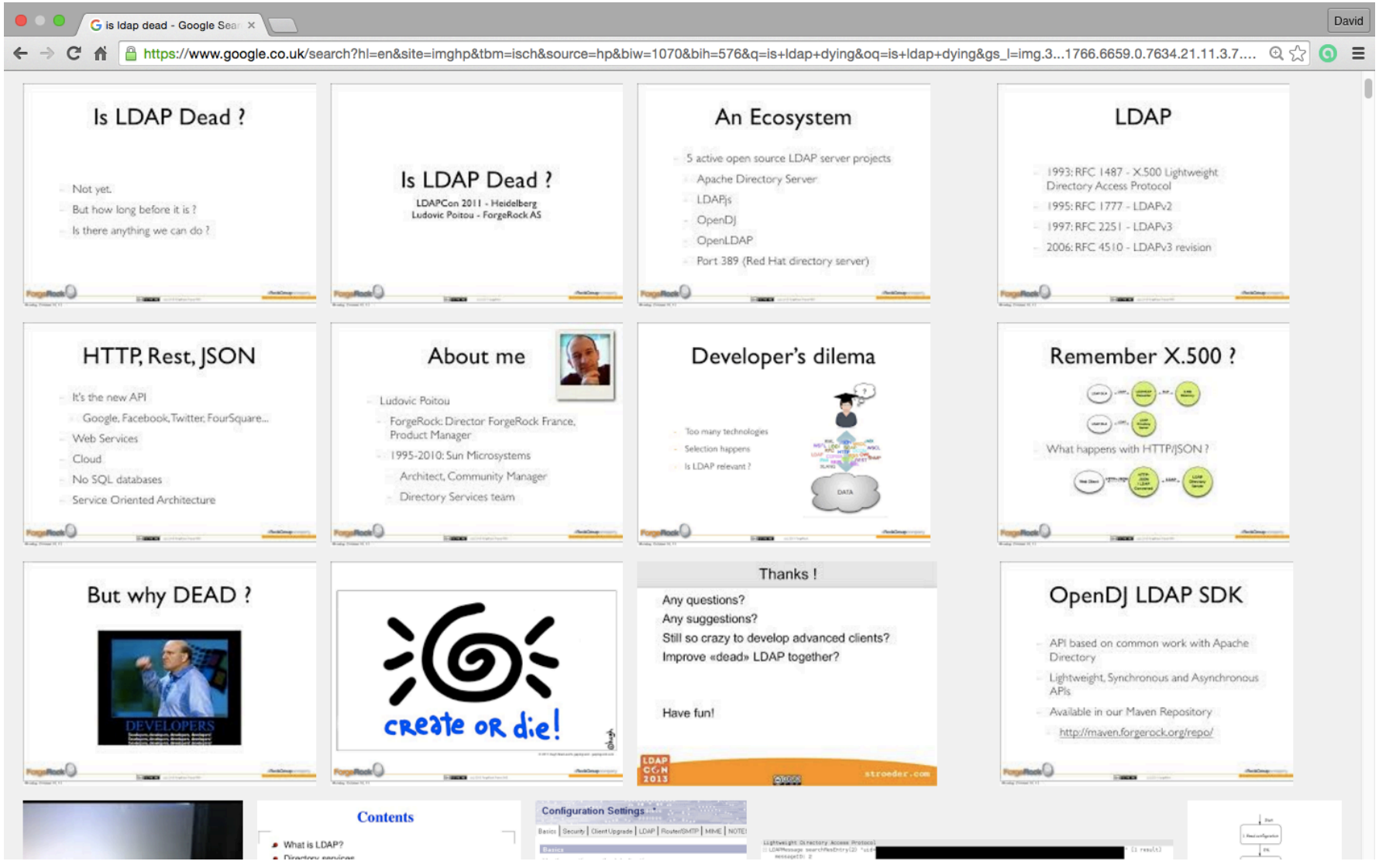
The №1 Consulting Agency

LDAP 2020:
Paradise Lost or Regained?

David Goodman, The No.1 Consulting Agency

12 November ‘15


is ldap dead - Google Sear
David
https://www.google.co.uk/search?hl=en&site=imghp&tbm=isch&source=hp&biw=1070&bih=576&q=is+ldap+dying&oq=is+ldap+dying&gs_l=img.3...1766.6659.0.7634.21.11.3.7....
Is LDAP Dead ?
Not yet.
But how long before it is ?
Is there anything we can do ?
Is LDAP Dead ?
LDAPCon 2011 - Heidelberg
Ludovic Poitou - ForgeRock AS
An Ecosystem
5 active open source LDAP server projects
Apache Directory Server
LDAPjs
OpenDJ
OpenLDAP
Port 389 (Red Hat directory server)
LDAP
1993: RFC 1487 - X.500 Lightweight Directory Access Protocol
1995: RFC 1777 - LDAPv2
1997: RFC 2251 - LDAPv3
2006: RFC 4510 - LDAPv3 revision
HTTP, Rest, JSON
It's the new API
Google, Facebook, Twitter, FourSquare...
Web Services
Cloud
No SQL databases
Service Oriented Architecture
About me
Ludovic Poitou
ForgeRock: Director ForgeRock France, Product Manager
1995-2010: Sun Microsystems
Architect, Community Manager
Directory Services team
Developer's dilema
Too many technologies
Selection happens
Is LDAP relevant ?
DATA
Remember X.500 ?
What happens with HTTP/JSON ?
But why DEAD ?
DEVELOPERS
create or die!
Thanks !
Any questions?
Any suggestions?
Still so crazy to develop advanced clients?
Improve «dead» LDAP together?
Have fun!
LDAP CON 2013
stroeder.com
OpenDJ LDAP SDK
API based on common work with Apache Directory
Lightweight, Synchronous and Asynchronous APIs
Available in our Maven Repository
http://maven.forgerock.org/repo/
Contents
What is LDAP?
Configuration Settings

Identify Yourself, Sir!

The №1 Consulting Agency

1990-94	University College London	PARADISE & PASSWORD EC projects
1994-2000	Lotus Development/ IBM Corp.	Domino Directory (Notes Name & Address Book)
2000-01	Metamerge AS	Bus-based integration middleware
2001-05	IBM Websphere/Tivoli	IBM Directory & Directory Integrator
2005-06	Identitas	
2006-12	Apertio/ Nokia Siemens Networks	One-NDS
2012-14	Ericsson AB	CUDB (Centralised User Database)
2014-	The No.1 Consulting Agency/ KuppingerCole	

The №1 Consulting Agency

Durante degli Alighieri, simply called **Dante**, born 1265 and died 1321, was a major Italian poet of the late Middle Ages. His Divine Comedy, originally called Comedìa and later christened Divina by Boccaccio, is widely considered the greatest literary work composed in the Italian language and a masterpiece of world literature.

The Divine Comedy describes Dante's journey through Hell, Purgatory, and **Paradise**. His depictions of Hell, Purgatory, and Heaven have provided inspiration for a large body of Western art, and are cited as an influence on the works of John Milton, Geoffrey Chaucer, William Shakespeare, and Lord Alfred Tennyson, among many others.

John Milton (9 December 1608 – 8 November 1674) was an English poet, polemicist, man of letters, and a civil servant for the Commonwealth of England under Oliver Cromwell. He wrote at a time of religious flux and political upheaval, and is best known for his epic poem Paradise Lost, written in blank verse. Milton followed up **Paradise Lost** with its sequel, **Paradise Regained**

The №1 Consulting Agency

In the beginning (c. 1990) there was:

COSINE sub-project 2.1 (boring)

But it morphed into:

PARADISE (a lot more fun)

Piloting A ReseArchers' DIrectory Service for Europe

The object of the exercise was to demonstrate to the research community, the telcos and the rest of the world, that X.500 worked.

At the end of four years, we could honestly look back and say that the case for X.500 had been proven:

- 40 countries, 700 interconnected DSAs
- the telco community planning to take up the mantle
- the Fortune 500 companies seeing X.500 as the answer to their directory woes and shortcomings

BUT, PARADISE had also been the mid-wife to the birth of the Skinny Stack, the DIXIE Protocol (RFC 1249) and eventually in July 1993 the Lightweight Directory Access Protocol v1

The reason why LDAP was conceived was that the IT department responsible for the world's largest X.500 deployment at the University of Michigan were concerned that the DAP client was too cumbersome for the Mac and Windows clients the departmental administrators used.

The intention at that stage was for LDAP to enhance the quest for X.500 global domination

BUT, it didn't quite work out that way … and the next small step in LDAP's development which removed the requirement for X.500 altogether was pretty significant

The perilous Great Trek across the Rockies to the Golden State was a rags to riches story for three intrepid developers from Wisconsin

The №1 Consulting Agency

The world was in thrall when in 1996 Netscape, *the* Internet company du jour, announced that it was supporting LDAP.

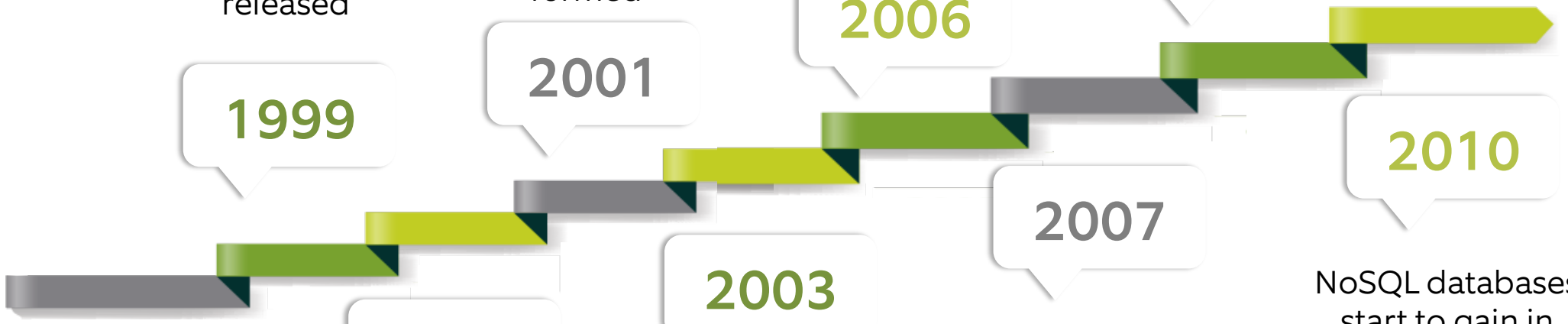
For several years all the major vendors had been forced to tell their customers (with forked tongue) how they were going to address X.500 without having a clue what to do ...

... and then relief came: simplicity and (finally) a workable API

X.500 was pronounced dead (or as good as) and then the following year came LDAPv3 and it was game over.

One Paradise Lost but another one Regained in the process

The №1 Consulting Agency



1998

OpenLDAP project starts and Symas founded (1999)

1999

DSML v1 approved; Open LDAP v2 released

2000

Active Directory released with Windows 2000 server

2001

Liberty Alliance formed

2003

Directory Plugfest with nine vendors; OpenLDAP 2.2 released

2006

RFC 45xx LDAP revision published; RFC 4533 Experimental (replication) published

2007

Ex-Sun employees found UnboundID; OpenLDAP 2.4 released
First LDAPCon!

2010

Oracle acquires Sun; Ex-Sun employees found ForgeRock

2010

NoSQL databases start to gain in popularity; Second (2009) and Third (2011) LDAPCon

Fortunately

The №1 Consulting Agency

LDAP is the de facto standard for most company enterprise directories – not least because Windows Server Active Directory supports LDAP – and change will be slow if at all

Most if not all of the major vendors (Oracle, IBM, ForgeRock, CA, Microsoft) have LDAP-based directory solutions

LDAP has achieved a level of maturity and familiarity with services organisations that make it relatively attractive to install and maintain

Unfortunately

The №1 Consulting Agency

Azure AD doesn't support LDAP although Windows Server Active Directory continues to do so – identity data likely to be passed as an object in a SAML message.

As the demands on database technology scale with aspirations for greater data consolidation and 'big data', architects are looking at the new kids on the block such as Hadoop, MongoDB, Cassandra, and NoSQL key-value stores and graph databases

Application developers are looking at APIs other than LDAP e.g., JSON, XML

Most if not all of the major vendors have a wide range of directory/database solutions, not just LDAP

Cloud

Cloud and cloud-based services are changing assumptions

- Monolithic directories are no longer satisfactory to service today's computing environment.

Exposing LDAP worked well when users were authenticated to a corporate network and any application accessing the directory could be trusted.

- In a Cloud environment, access can come from anyone, anywhere, While they may be retained as a "source of truth", applications and devices will need access to a readily accessible directory service – a cloud based repository of, at least some, identity information

Microsoft Azure will make the OData interface as ubiquitous as LDAP.

Performance

It is not appropriate to expose the corporate directory from a performance viewpoint.

- It is not realistic to expect a Cloud-based application to send a user lookup request to the corporate network, wait while the request punches though the firewall, transits the load balancer, and waits to get serviced.

Applications expect millisecond responses that require a planned configuration that reduces network latency to the utmost degree possible.

Access Control

Applications are moving to externalise their access control decision-making to an external “decision point” i.e. moving from a course-grained authentication to a fine-grained authorisation.

- As this occurs the identity repository will be embedded with a decision point as the source of attributes for access control policies

Application Development

The software development environment prefers to work with object-oriented languages and Internet protocols.

- Developers prefer JSON arrays and HTTP methods over LDAP Put and Get.
- To pull back multiple data points, and to use JSON arrays means that the directory must support a SAML request, perform the lookup and respond with the appropriate data points.

For basic UID look-ups programmers the HTTP GET method doesn't scale and can't satisfy anything but a simple query.

- An intelligent directory interface is required that can accommodate data joins and optimise lookup requests is required.

Standards

The use of standards is becoming more important (again).

- There is increasing pressure for standards such as SCIM (System for Cross Domain Identity Management) to be supported by an identity provider service.

There is growing interest in more complex “relationship” data to be retrieved by a directory lookup.

- A person look-up might want to retrieve organisations with which they do business or clubs they belong to or schools they attend.
- Increasingly directories are being required to adopt a more database approach with a “graph” operation rather than table lookup.

Federation

Federation has been an option since the ’90’s but with the growing interest in data consolidation and analytics (aka ‘big data’), virtual/ federated/meta- databases are very much in vogue.

The traditional enterprise LDAP directory is a component but little more and LDAP does not have a key role to play beyond it

The №1 Consulting Agency

Is LDAP dead?

No, LDAP is definitely not “dead”. Nor dying.

BUT challenges are apparent and real, particularly with the growth of Cloud

At the very least, it will continue to service on-premise applications that already have an LDAP interface

Postscript

During the **early '90s** a group of ex-GCHQ architects in Bath/ Bristol were building telco applications for Orange based on a home-grown relational database

By the **late '90s** they recognised that SQL was lacking and lighted on X.500 as the ideal solution for reading and writing very large core network data sets (from 1-200 million users) in real time (i.e., between 2-5 milliseconds)

Without thinking twice, they went away and built an X.500-based solution that did just that …

By **2004-5**, during early adoption, the product and the 'new' X.500/LDAP technology took the telco market by storm and created a move to consolidated 'next generation' distributed storage for the core networks

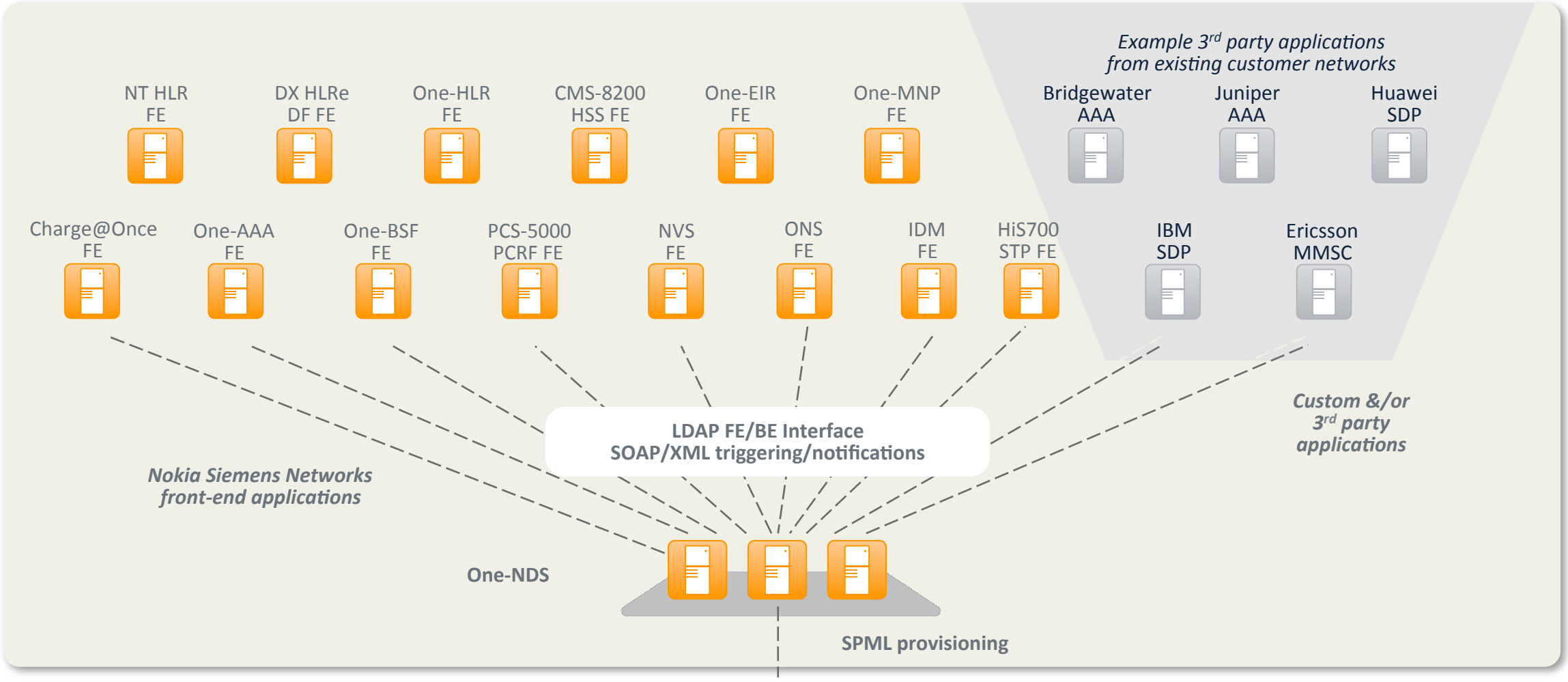
By **2010**, all the major suppliers of core network systems – Nokia, Ericsson, Huawei and Alcatel-Lucent – were replacing their legacy subscriber data management applications with LDAP-based back ends

By late **2015**, most of the world's operators are either live or are planning to go live

This equates to roughly **four-five billion** subscriber records …

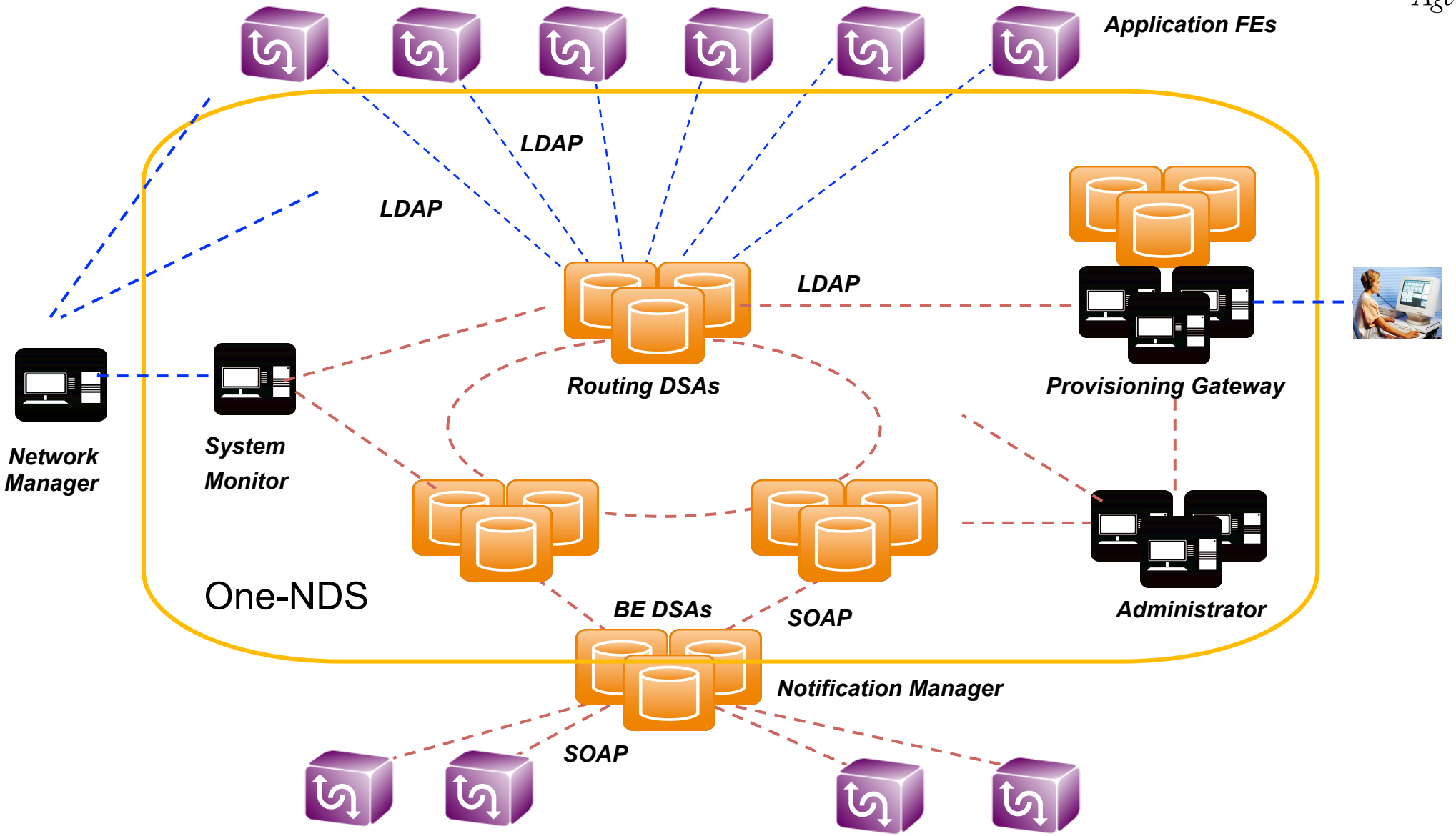
This is suitably ironic as X.500 was originally intended for … telcos.

Subscriber Data Management (Nokia)

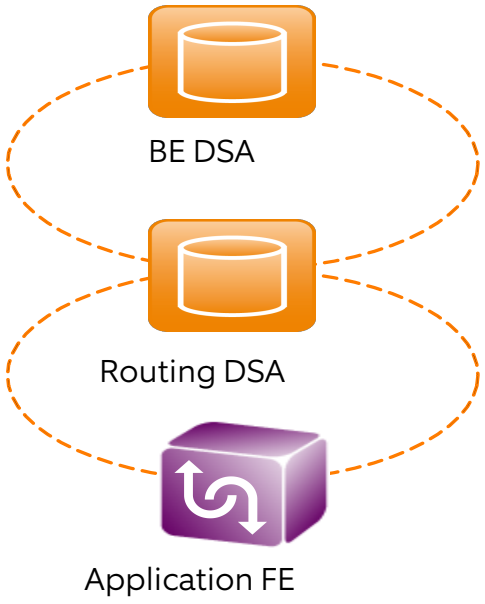


One-NDS Architecture

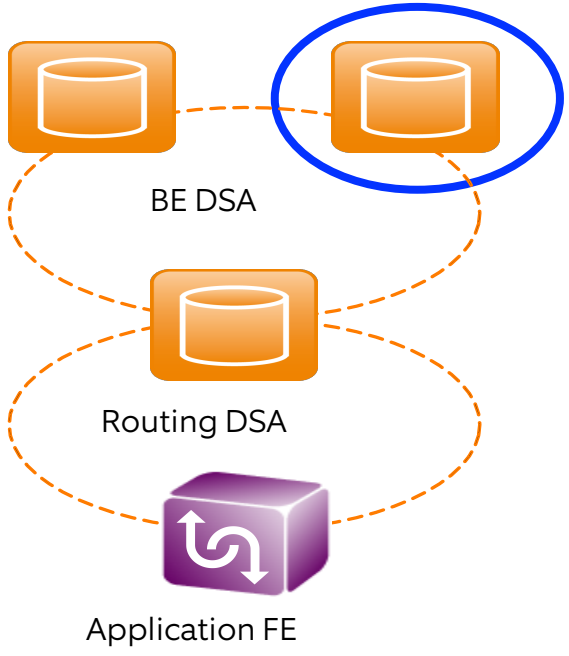
The №1 Consulting Agency



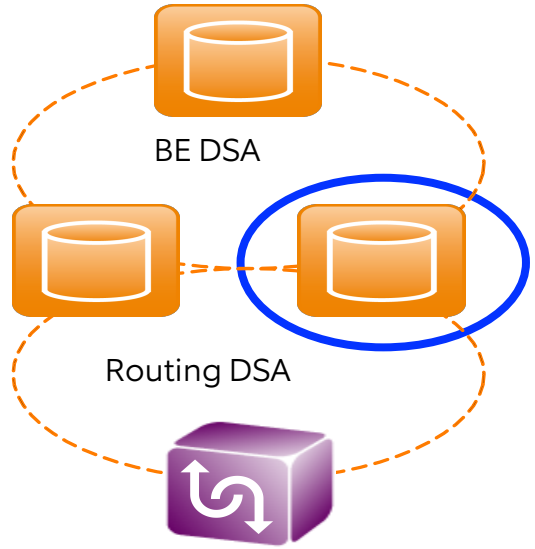
Transparent Scalability



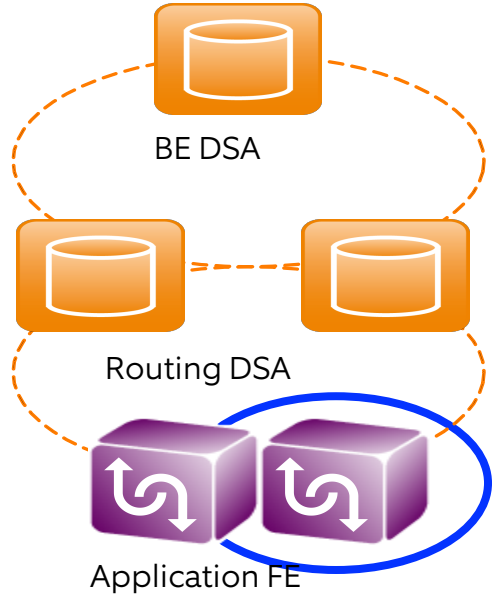
Decoupled Architecture



Increased Data Capacity



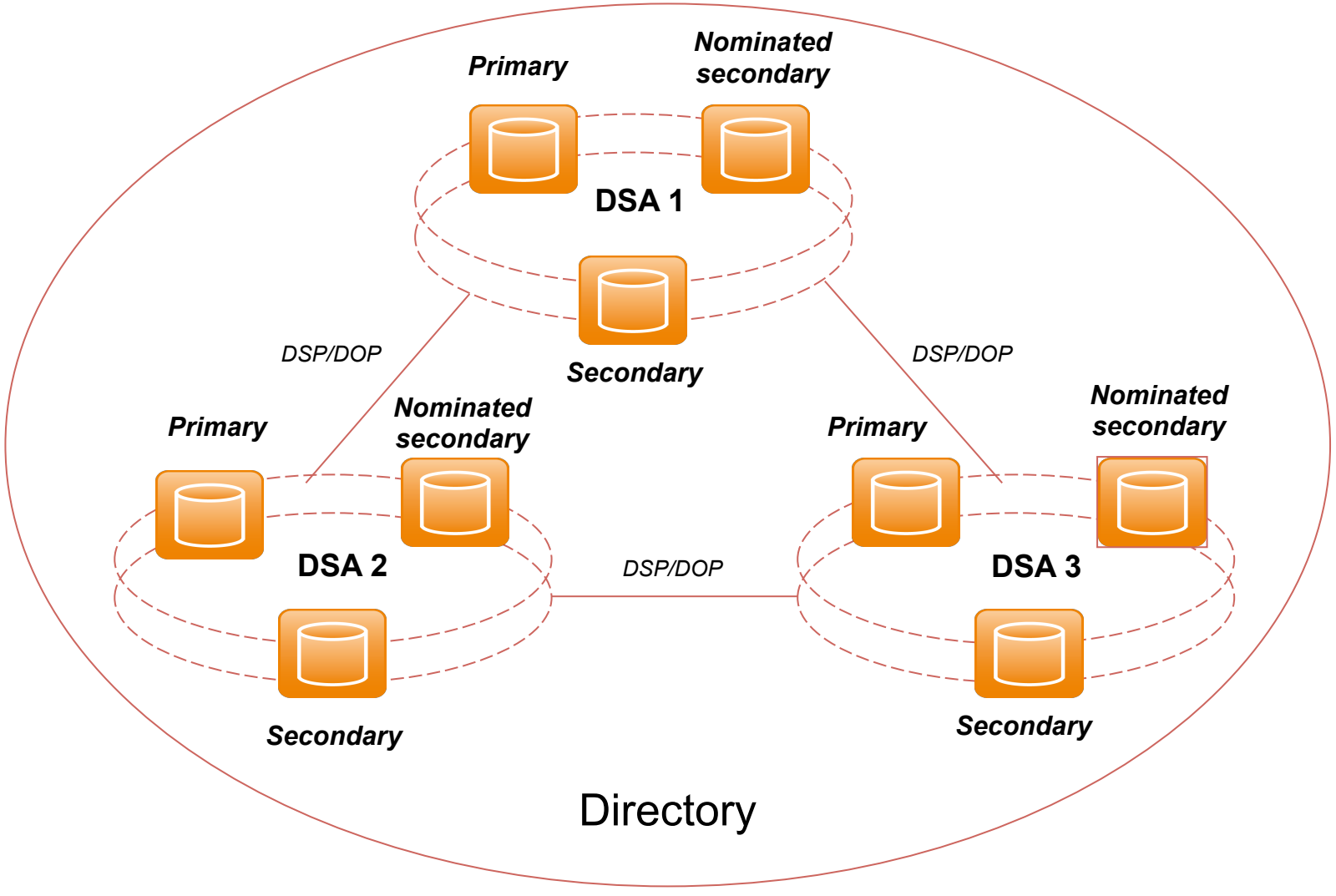
Increased ID Capacity



Increased Transaction Capacity

Dual independent scalability
Add more Back Ends for data capacity
Add more Front Ends for transaction capacity
Scalability transparent to live deployment

DSA Distribution

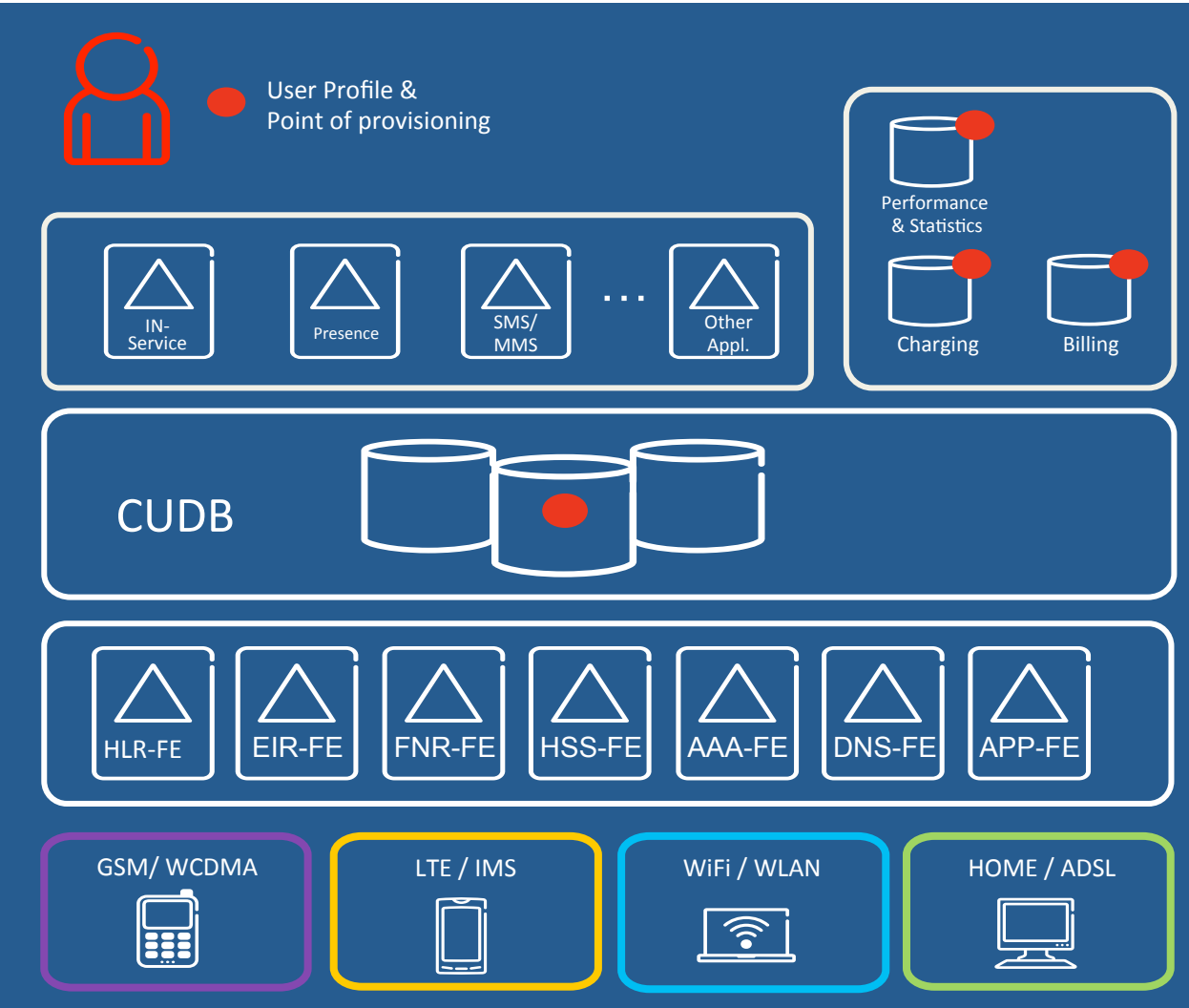


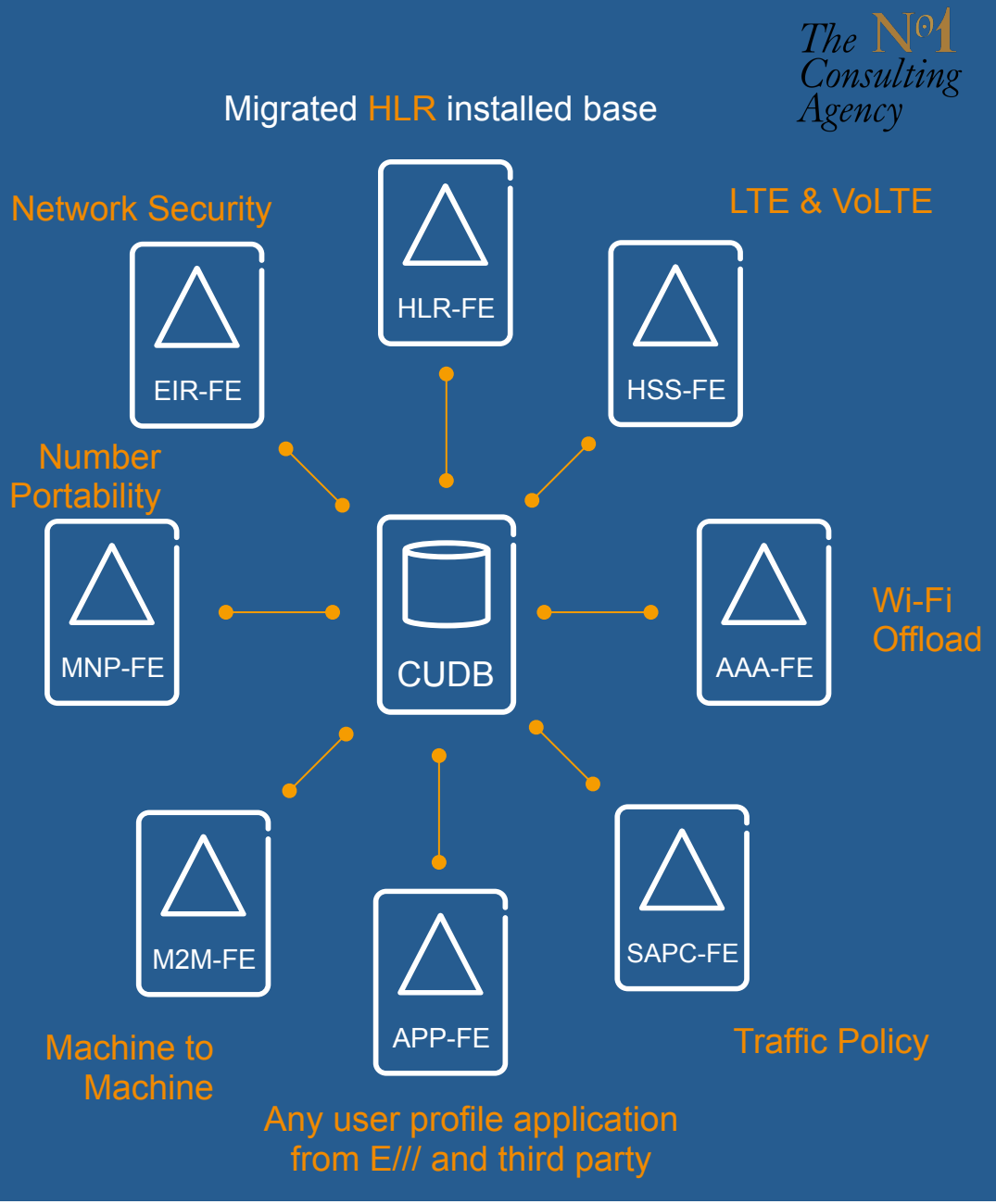
The №1 Consulting Agency

Beyond the LDAP RFCs …

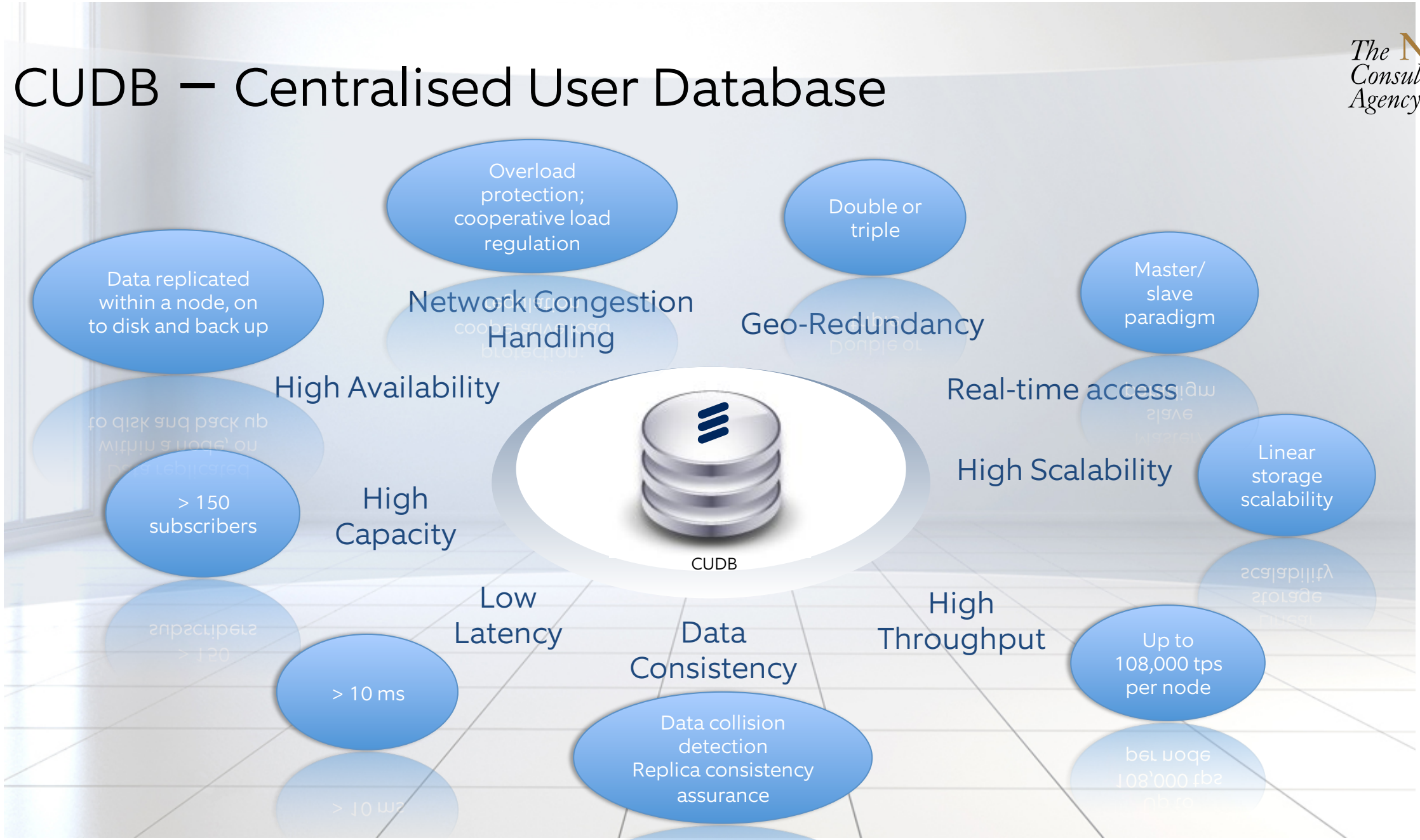
- Replication
- Transaction support
- Common data model
- Schema adaptation
  - Aliases and alias hiding, variant entries, adaptive naming, attribute adaptation
- Multi-tenancy

User Data Management (E///)





CUDB – Centralised User Database



Key Values and Benefits

Single point of data access and store

- Subscriber data accessible from any node in the system
- Consolidated data model for many applications

High performance, high availability

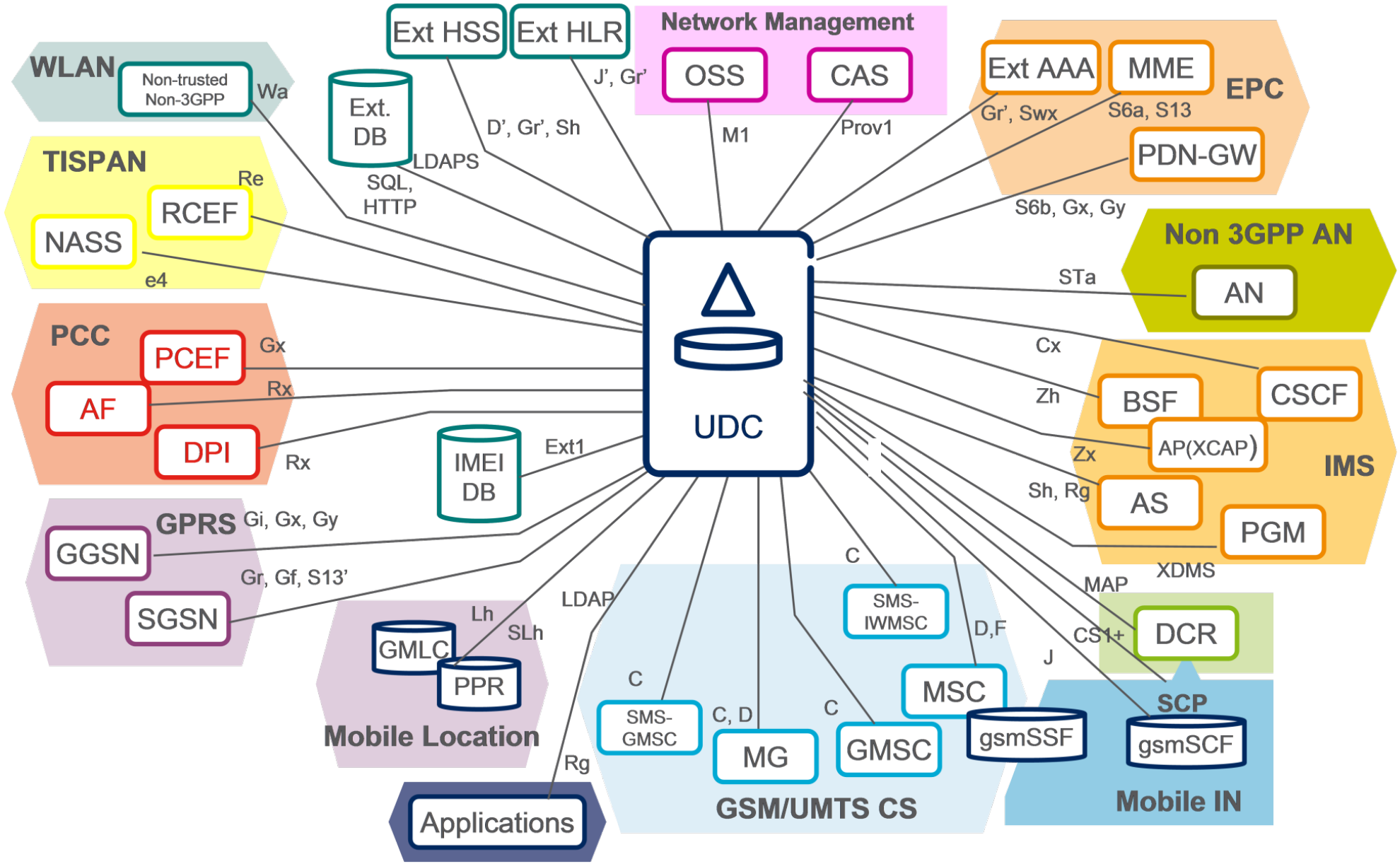
- Telecom grade performance and characteristics
- Non interfering access to network data
- Simplified monitoring of real-time changes in subscription data
- Efficient geographical redundancy

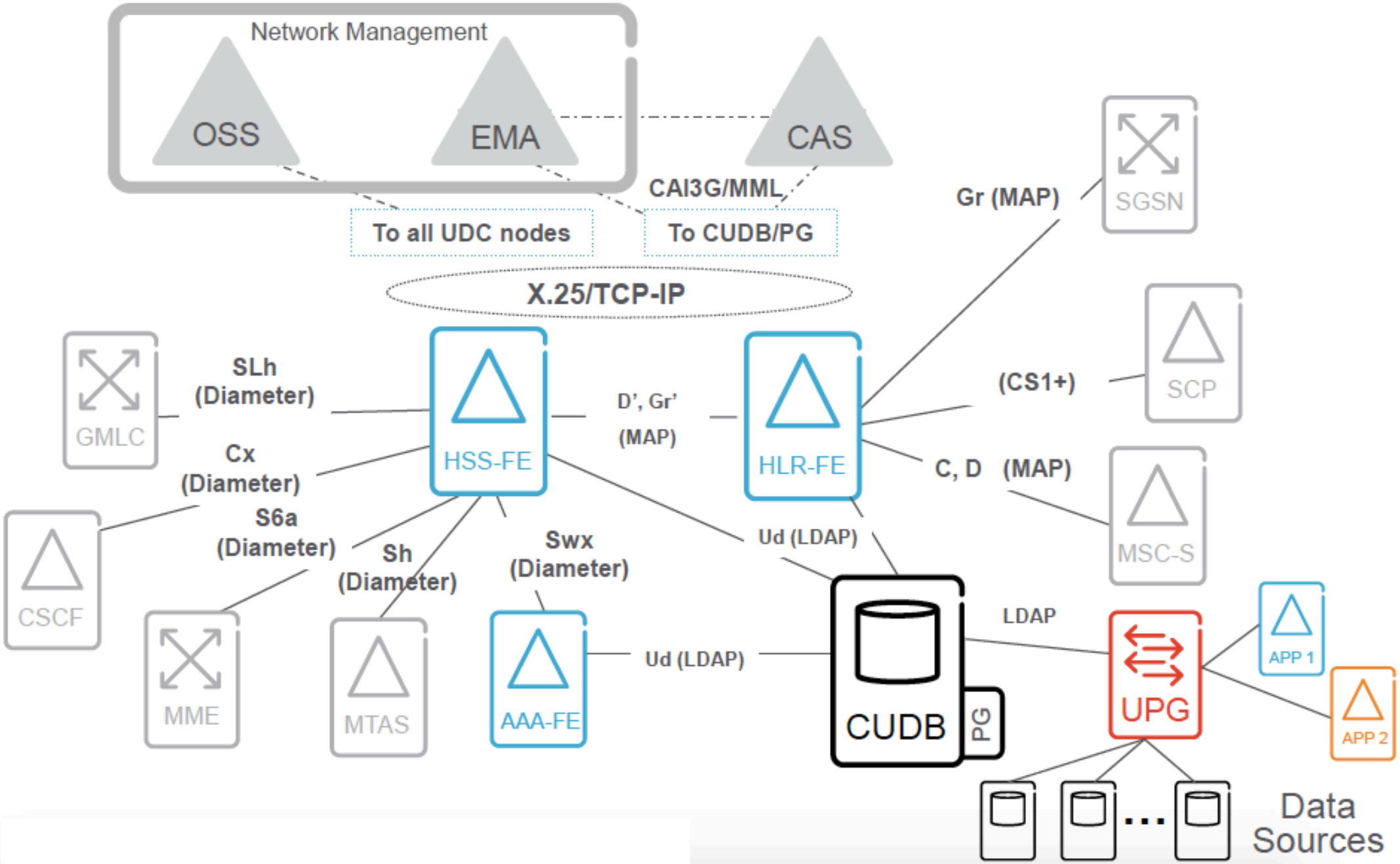
Compliance to 3GPP standard, use of open protocols

- Future proof investment and evolution
- Less need for customizations
- Standard protocols simplifies integration towards rest of network

Data model extensibility, linear scalability

- Extension of data model without service disruption
- Simplified introduction of new services in a network
- Integration of new / different application front ends
- Optimal dimensioning of processing and data storage resources





The moral of this tale is that the world is full of surprises!
Don’t lose faith, focus on core strengths and don’t underestimate the competition.

The №1 Consulting Agency

PARADISE

Neither lost nor regained
It never went away
And it’s here to stay (probably)

The №1 Consulting Agency

Thank you!

david@theno1consultingagency.com
david27501
www.theno1consultingagency.com