

## SERAS – A REST API For Directory Access

by Horst Fuhrmann and Alex Belousov

NetIQ eDirectory previously owned by Novell, also known as Novell Directory Services (NDS) and sometimes referred to as NetWare Directory Services was initially released by Novell in 1993 for Netware 4. eDirectory is a full-service, secure LDAP directory providing scalability and an agile platform to run an organization's identity infrastructure and services. It is an X.500-compatible directory service and can be accessed via the following interfaces:

- NDAP (Novell Directory Access Protocol)
- LDAP (Lightweight Directory Access Protocol)
- DSML (Directory Services Markup Language)
- SOAP (Simple Object Access Protocol)
- ODBC (Open Database Connectivity)
- JDBC (Java Database Connectivity)
- JNDI (Java Naming and Directory Interface)
- ADSI (Active Directory Service Interface).

This is quite a number of different interfaces and hence fully covers *traditional* client needs, but it does not help much in today's mobile world. Most new devices like Apple, Android and Chrome phones and tablets are designed for use with http/https protocols and nothing else.

### How mobile devices and web application access data - The Rise of the REST API

Since these new mobile devices were solely designed for http/https protocols many people were searching for methods that allow to marry the 2 universes of business applications and consumer devices. As it turns out the solution for this problem is the REST (Representational State Transfer) protocol.

REST is nothing new, it is based on pretty old scientific work, which describes some basic principles. Representational State Transfer or REST is an architectural style that sets certain constraints for designing and building large-scale distributed hypermedia systems. As an architectural style, Representational State Transfer has very broad application. The designs of both HTTP 1.1 and also URIs follow RESTful principles.

### The Birth of REST: Roy Fielding's Dissertation

In 2000, Roy Fielding and his colleagues had one objective: create a standard so that any server could talk to any other server in the world. In his doctoral dissertation<sup>1</sup> he came up with the Representational State Transfer (REST).

1. Roy Thomas Fielding, 2000: PhD dissertation, Chapter 5 Representational State Transfer (REST)  
[www.ics.uci.edu/~fielding/pubs/dissertation/rest\\_arch\\_style.htm](http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm)

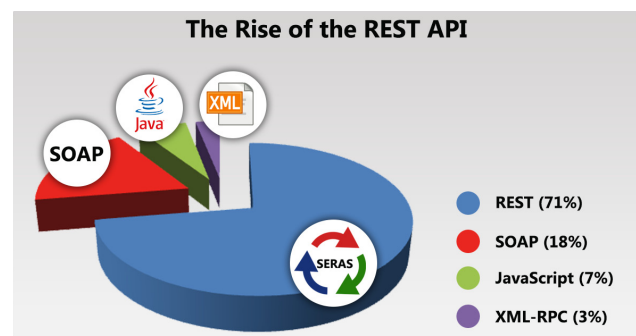


Figure 1: REST APIs are predominant today

Roy Fielding wrote: "I had comments from well over 500 developers, many of whom were distinguished engineers with decades of experience, and I had to explain everything from the most abstract notions of Web interaction to the finest details of HTTP syntax. That process honed my model down to a core set of principles, properties, and constraints that are now called REST.

- Uniform interface.
- This means we always use HTTP verbs (GET, PUT, POST, DELETE).
- We always use URIs as our resources.
- We always get an HTTP response with a status and a body.
- Stateless - this means each request is self-descriptive, and has enough context for the server to process that message.
- Client-server - there has to be clear boundaries between roles of the two systems. One server, operationally, has to function as the server that is being called and the other has to function as the one making the requests.
- Cacheable - unless denoted, a client can cache any representation.

This is possible thanks to the statelessness—every representation is self-descriptive."

REST is an architecture for distributed applications using WEB technologies. The World Wide Web is no doubt the largest and best known REST application. Many other web services also follow the REST architectural style.

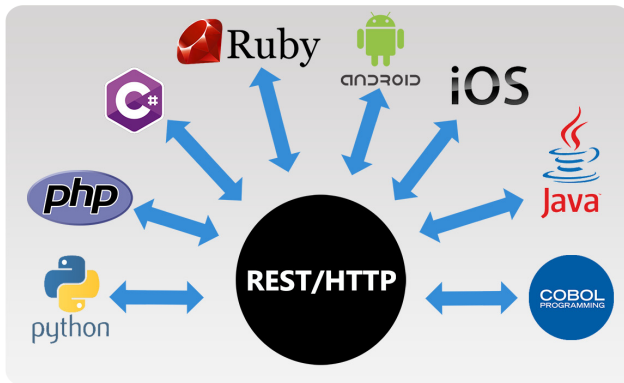


Figure 2: REST is a central feature of the WWW

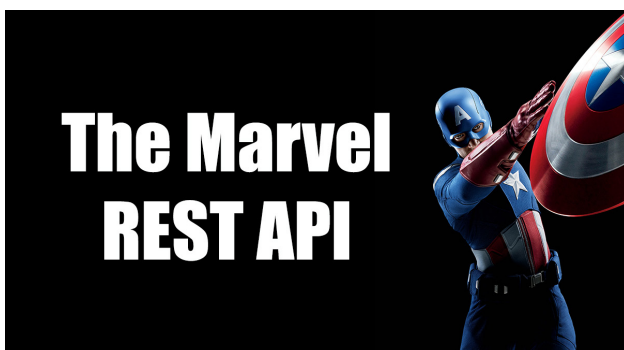
### What are the advantages of a REST API

The main advantages of REST web services are:

1. Lightweight - the requests and responses can be short.
2. Human Readable Results - flexible & simple, URIs for identification.
3. Easy to build - No toolkits required.
4. Totally stateless operations - stateless CRUD (Create, Read, Update, and Delete) operations.
5. Caching situations - information can be cached because of the totally stateless operation.
6. Many vendors are developing their own APIs based on the REST specification.

Google, LinkedIn, Twitter, Amazon, Facebook, Oracle, Microsoft are just a few names of the big players in this area.

Microsoft uses the Graph API for managing the Azure and Office 365 Cloud. Other big players like Cisco, HP, Dell include RESTful API services on their own hardware for support purposes. Even MARVEL have created a REST API for their own comic characters.



### The SKyPRO Enhanced REST API Service (SERAS) - SKyPRO's REST to LDAP Gateway

SKyPRO started to develop an interface for accessing eDirectory data, because one of our customers wanted to synchronise an external application (3rd Party) with existing eDirectory data. We were looking for simple ways that would allow our customer to access this data over a highly secure channel. We were also looking for ways to have a generic access that could easily be adapted to any future requests or possible change request.

Hence, SERAS was based on REST and implemented in way that would allow to easily reconfigure it for most customer requests and applications. It was also clearly geared for agile development and microservices. The microservice architecture enables continuous delivery and deployment of large and complex applications.

- SERAS make it easy to develop and expose REST APIs for any LDAP based data serve.
- SERAS were originally built as a highly resilient and scalable cluster-aware system.
- RESTful APIs that can be readily accessed by any development language without requiring any driver software to be installed.

All modern languages and even legacy languages such as COBOL and Fortran support HTTP/HTTPS and hence REST out of the box.

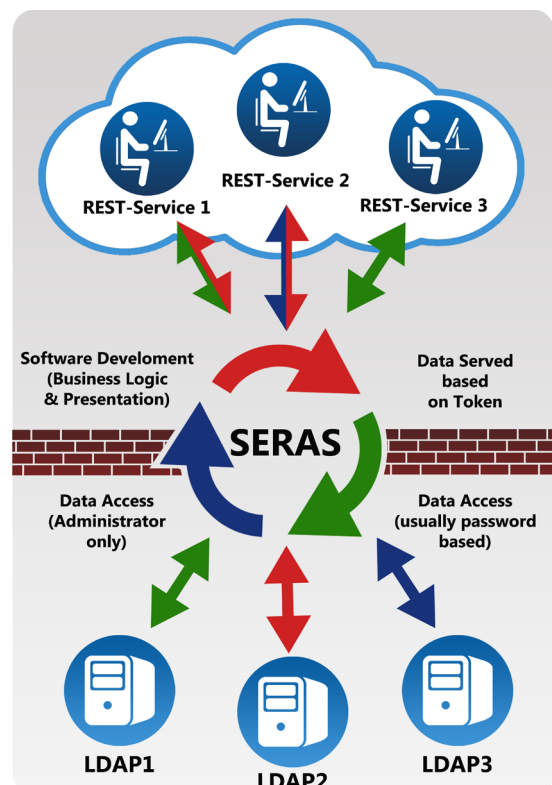


Figure 3: SERAS architecture

About a month ago Alex received a request from within the company that they need an iPhone application for accessing user information from their internal Enterprise Directory Server (LDAP/eDirectory). He started to look for applications that are currently available on the market that could be used as a REST gateway. He reviewed a number of applications but has selected SERAS (SkyPRO Enhanced REST API Services).

Alex has worked closely for a few years with SKyPRO and has a good knowledge of our product line. SKyPRO's Enhanced REST API Services have an exceptional architecture and number of unique functions that distinguishes them from similar products.

- On top of standard ACL mechanisms, SERAS added a number of extra unique security layers.
- One SERAS instance can serve an unlimited number of LDAP data sources at the same time.
- Different applications can use dedicated profiles with their own, application specific settings and parameters.
- SERAS has a native Elasticsearch integration.
- The highlight of SERAS is the ability to query and result documents through input/output transformation scripts (something similar to IDM Input/Output Transformation Policy).
- Additional transformation Javascript functions can be added to the functional libraries.

### SERAS: A closer look

Let's start and configure SERAS

1. Start from command line start. **sh / start.cmd file.** (figure 4)
2. Connect to the Service via `http://localhost:8182`. You will see an initial web page that will look as shown in figure 5.
3. The service configuration page may look like figure 6 (over page).

```

$ java -jar SERAS-1.0.3-jar-with-dependencies.jar
Connected
2017-08-30 13:17:30.909 INFO      Admin Server: Starting Rest Admin Service
2017-08-30 13:17:30.916 INFO      Admin Server: Starting Component on Port 8182
2017-08-30 13:17:30.916 INFO      Admin Server:   Contains App: Admin_Server
2017-08-30 13:17:30.932 INFO      Admin Server: Logging initialized @357ms
  
```

Figure 4: SERAS command line start

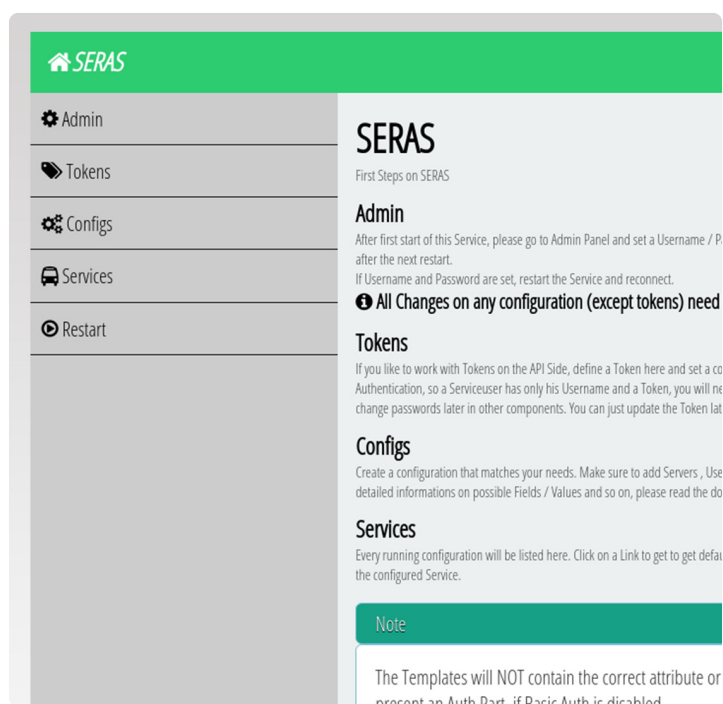


Figure 5: Screenshot of initial SERAS web page

4. A few important parameters to consider for configuration
  - a. Start by using the preconfigured tokens instead of any passwords.
  - b. If checked, the server will accept tokens, and lookup matching tokens in his List.
  - c. Replace a token at runtime with a password.
5. Allow Loose Rights.
  - Do we allow Loose Rights? This means we don't need to add Attributes to the Config.
  - We allow all Attributes for Search / Retrieve and Modify
6. InputScript - JS Script to apply to input documents
7. OutputScript - JS Script to apply to output documents

### A Real life example

In our scenario, an iPad web application has to query user information based on known NT-logon information. This is a trivial task for any traditional LDAP client but it is an almost impossible objective for a regular mobile device. The task becomes even more complicated, because the application (for its own strange reasons) has its AD account information in a very strange and unusual format.

The application is unable to correctly handle the backslash character (\) and it is replaced with the hyphen (-). As a result, instead of receiving the account information in a format like `domain\samaccountname` it has the information in format `domain-`

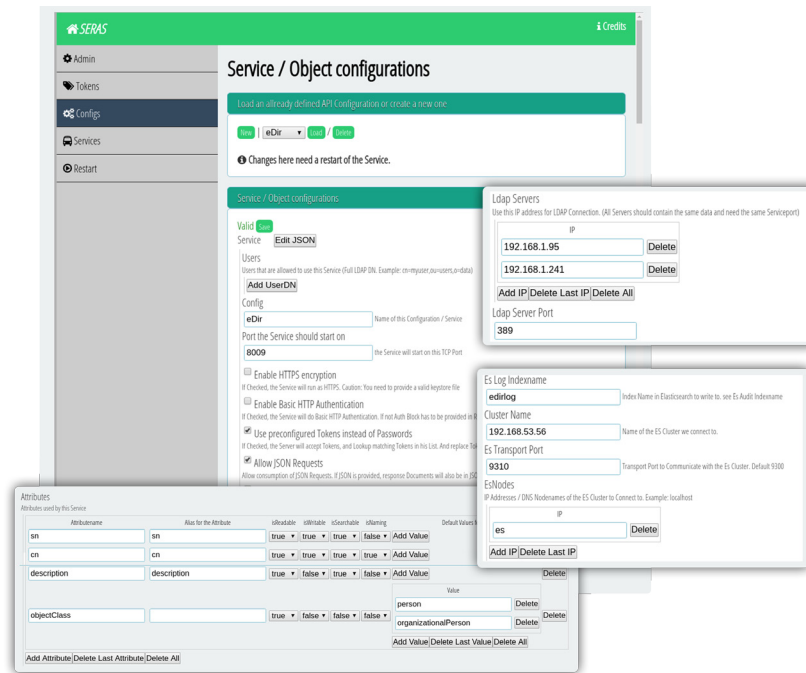


Figure 6: SERAS service configuration

samaccountname. The LDAP server has the NT-Logon information available in the correct format.

Making the appropriate data format changes usually requires necessary adaptations on the application side (that potentially can have negative impact on other parts of the

application). Changing the application code, in order to accommodate these changes is not always acceptable, especially when this is a purchased third-party application.

SERAS has the ability to execute real-time data transformation and has become a lifesaver in this situation.

Figure 7 demonstrates, in screenshots and logs from NetIQ Validator and iMonitor LDAP traces, a simulation of the application's behaviour. It shows that the application successfully received the required information. They show that the real LDAP query has the NT-Logon information in the correct format and it found the requested objects in the LDAP storage.

As a result we conclude that SERAS allows us to get the required results without any application code modification.

SERAS is a flexible tool and will give you simple ways to achieve your desired goals without huge investment and the rebuilding of your existing applications.

**Horst Fuhrmann** is CEO of SKyPRO, the Swiss based company he founded in 1987, focused on developing communications and IDM solutions. Horst's background is in mechanical engineering and physics.

**Alex Belousov** is originally from Belarus, but now lives in Toronto, Canada. He's worked with Novell technology since the days of NW3.11. Since 2004 he's been immersed in the exciting IDM world, latterly as an Enterprise Directory Planner.

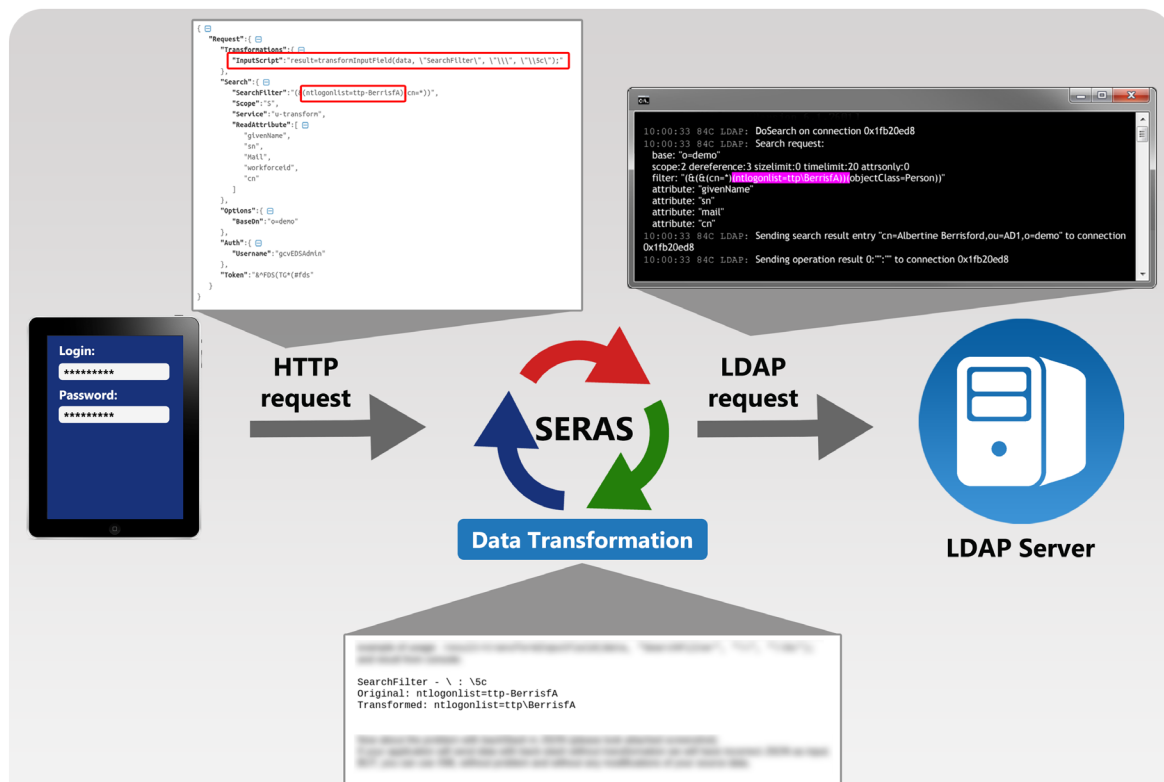


Figure 7: SERAS in action - logs from NetIQ Validator and iMonitor