



# Jurassic SAP

Juan Perez-Etchegoyen  
[jppereze@onapsis.com](mailto:jppereze@onapsis.com)  
[@jp\\_pereze](https://twitter.com/jp_pereze)

Sergio Abraham  
[sabraham@onapsis.com](mailto:sabraham@onapsis.com)  
[@serj\\_ab](https://twitter.com/serj_ab)



*This presentation contains references to the products of SAP AG. SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world.*

*Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius and other Business Objects products and services mentioned herein are trademarks or registered trademarks of Business Objects in the United States and/or other countries.*

*SAP AG is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.*

**Transforming how organizations protect the applications that manage their business-critical processes and information.**

- **Founded:** 2009
- **Locations:** Buenos Aires, AR | Boston, MA | Berlin, DE | Lyon, FR
- **Technology:** Onapsis X1 (Auditor Solution)  
Onapsis Security Platform (Enterprise Solution)  
(PCT patent-pending)
- **Pricing:** Subscription-based (Enterprise, Audit On-Demand and MSP)
- **Research:** 200+ SAP security advisories and presentations published



# Who are We?



- Juan Perez-Etchegoyen (JP) – CTO @ Onapsis
  - Background on Penetration Testing and vulnerabilities research
  - Reported vulnerabilities in different SAP and Oracle Products
- Sergio Abraham – SAP Security Specialist @ Onapsis
  - Reported vulnerabilities in different SAP Products
  - Worked on the support of HANA in Onapsis products
- Both Authors/Contributors on diverse posts and publications
- Speakers and Trainers at Information Security Conferences



- Introduction
- Use Cases
- Architecture
- Attack surface
  - Discovery
  - Technical Information Gathering
  - Business Information Gathering
- Conclusions

# SAP TREX

TREX =  
Text Retrieval and information Extraction

... It's a Search Engine!

- ❑ TREX 7.0 -> TREX 7.1
- ❑ Standalone engine, can be used by SAP Netweaver ( unique SAP SID, SAP SysNr)
- ❑ Support for complex and distributed environments
- ❑ It is a Search and Classification Engine + Text Mining Services

- ❑ Search in:

- Unstructured data
- Structured data
- Full text
- Attributes



- ❑ Search modes:

- Exact
- Linguistic: stemming, etc
- Fuzzy: Search error tolerant
- Wildcards and truncations
- Boolean operators
- Federated Search



- ❑ First code written in 1998
- ❑ TREX became an SAP component in 2000
- ❑ Integrated as the SAP NetWeaver BI Accelerator in 2005.
- ❑ SAP Netweaver Enterprise Search 7.0 in 2008
- ❑ ...
- ❑ Currently:
  - ❑ SAP TREX release 7.1.
  - ❑ SAP Netweaver Enterprise Search release 7.3

## □ Why using SAP TREX?

- A scan of 10,000 documents could take hours
- A scan of an index of 10,000 documents could take seconds
- SAP Systems have **thousands of business objects and documents**
- Querying on these large sets of data could take a long time
- **Indexing** all possible business objects and documents **within the database is not an option**
- **Conclusion:** we want indexes but we can't index.
- **Solution: SAP TREX**
  - **Asynchronous and separate index engine so support searches across SAP systems**

SAP systems store and process the most critical business information in the Organization. If the SAP platform is breached, an intruder would be able to perform different attacks such as:

- **ESPIONAGE:** Obtain customers/vendors/human resources data, financial planning information, balances, profits, sales information, manufacturing recipes, etc.
- **SABOTAGE:** Paralyze the operation of the organization by shutting down the SAP system, disrupting interfaces with other systems and deleting critical information, etc.
- **FRAUD:** Modify financial information, tamper sales and purchase orders, create new vendors, modify vendor bank account numbers, etc.

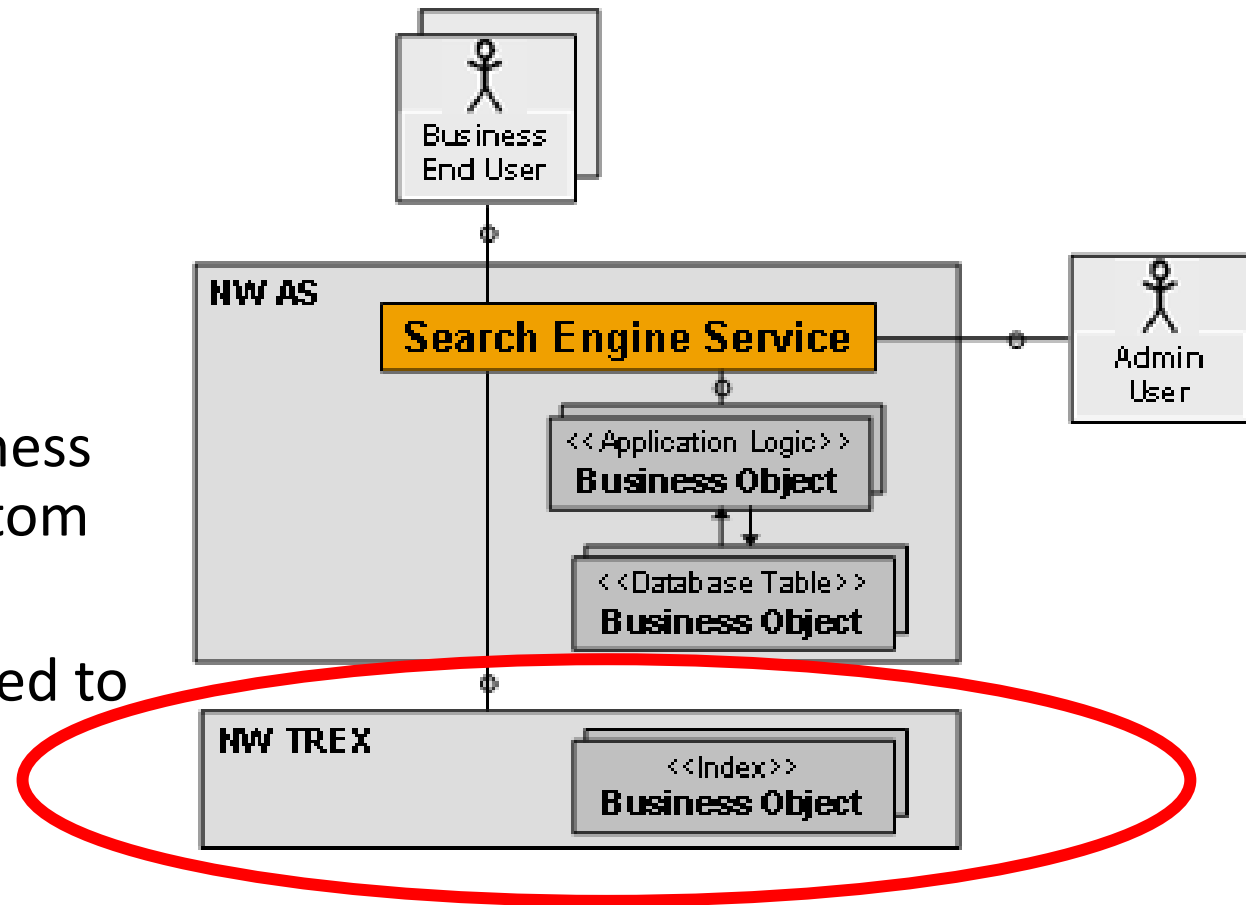
# Use Cases

# SAP TREX | Use Case 1



## ❑ Search Engine Service

- Index and Search Technology
- It is a layer on top of SAP TREX
- Used for SAP business objects
- Configured using tx SES\_ADMIN
- Commonly used in: **F4**
- Actually it has more than 50 business object types implemented, but custom objects can be easily included
- Indexing and Searching is restricted to one SAP System

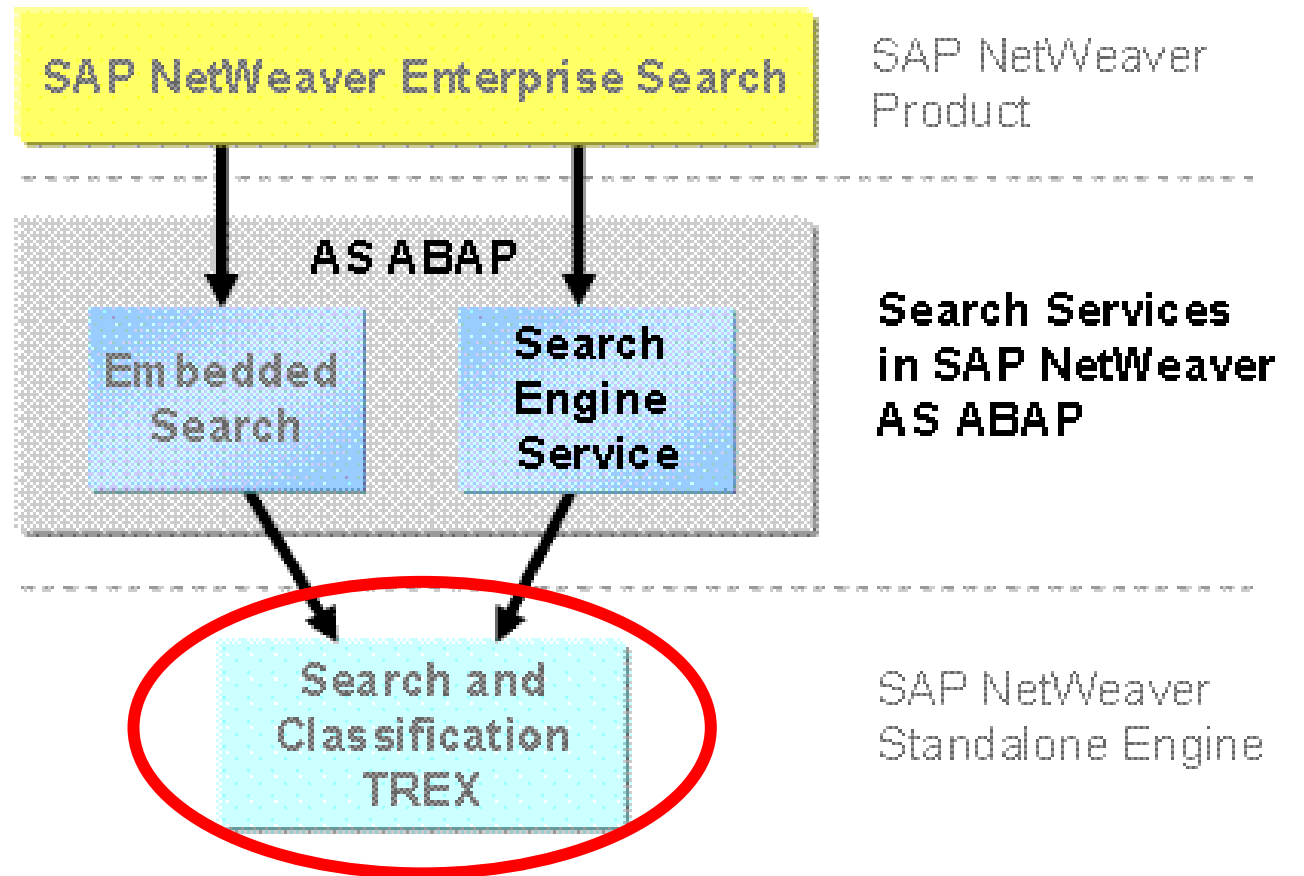


# SAP TREX | Use Case 2



## ❑ SAP Netweaver Enterprise Search

- Search Solution
- It is layer on top of the Search Services in SAP Netweaver AS ABAP (**Search Engine Service** and **Embedded Search**)
- It extends the range of search to more than one single SAP System
- It can connect SAP and non-SAP systems as search providers

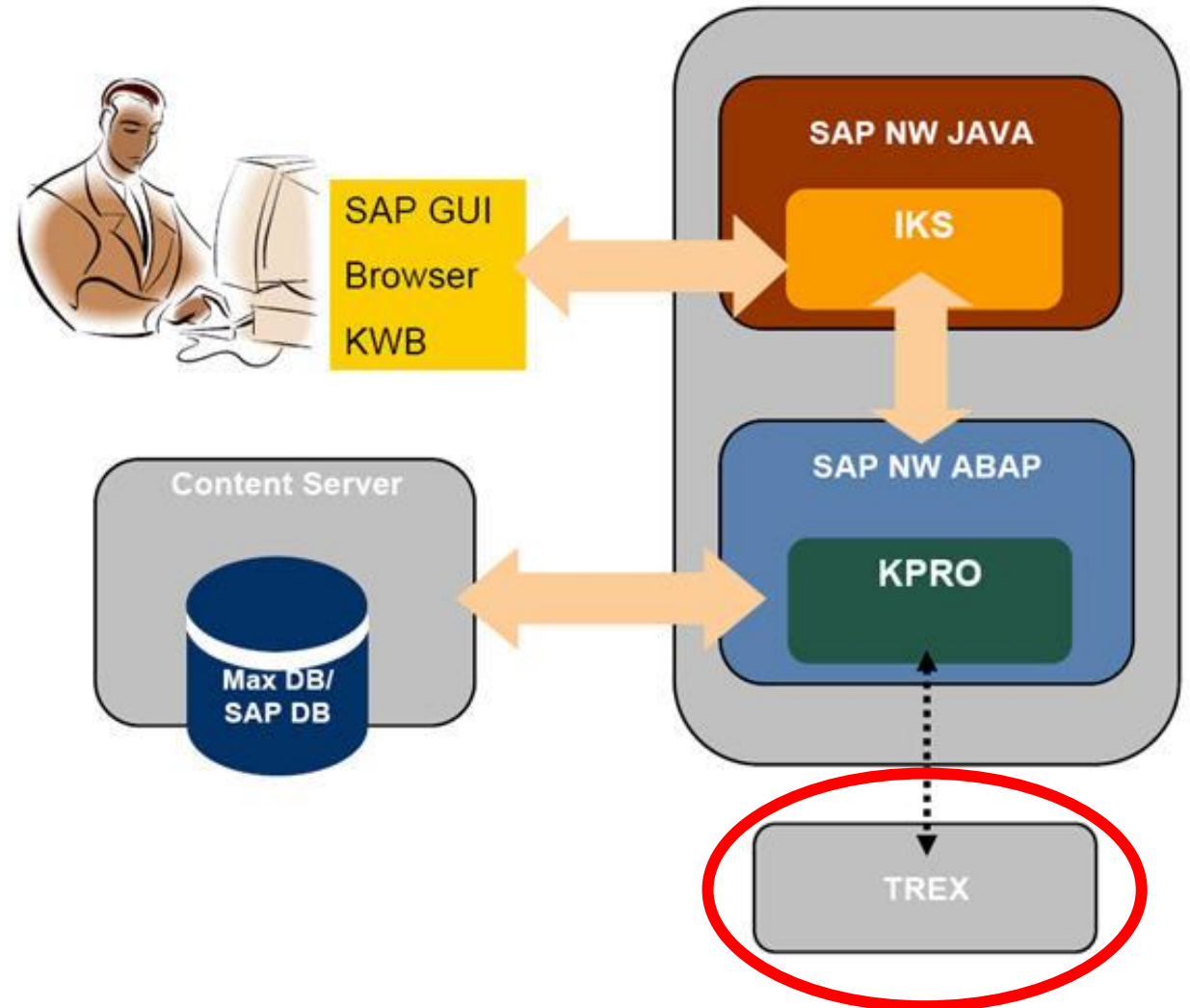




# SAP TREX | Use Case 3

## ❑ SAP Knowledge Warehouse

- Knowledge Management Solution
- Manages own enterprise-specific knowledge (documentation, training materials, manuals)
- Provides authoring environment
- Robust version control

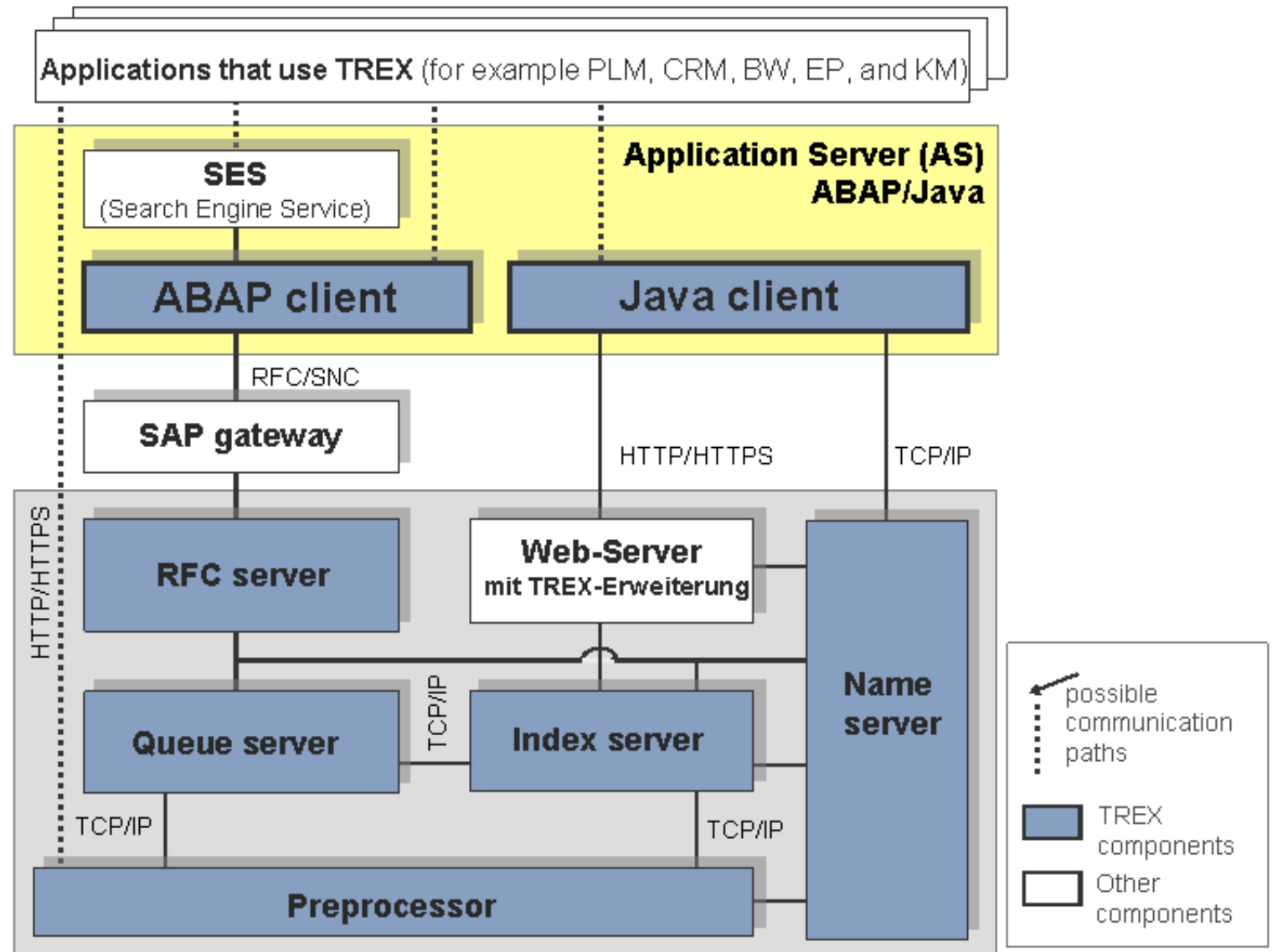


# Architecture

## Client-Server Architecture

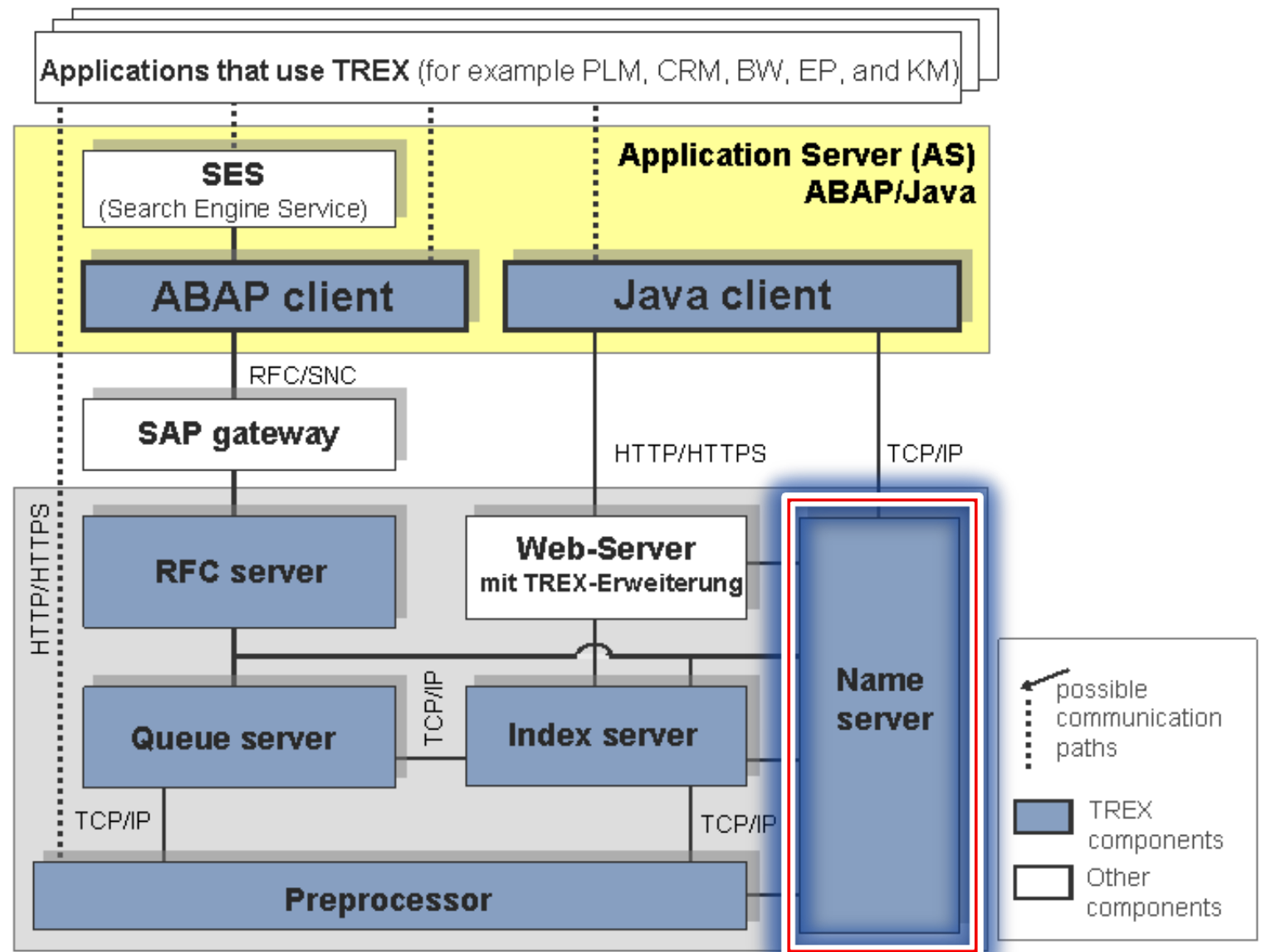
### Main components:

- Name server
- Index server
- Queue server
- Preprocessor
- RFC server
- Web server
- ABAP client
- Java client



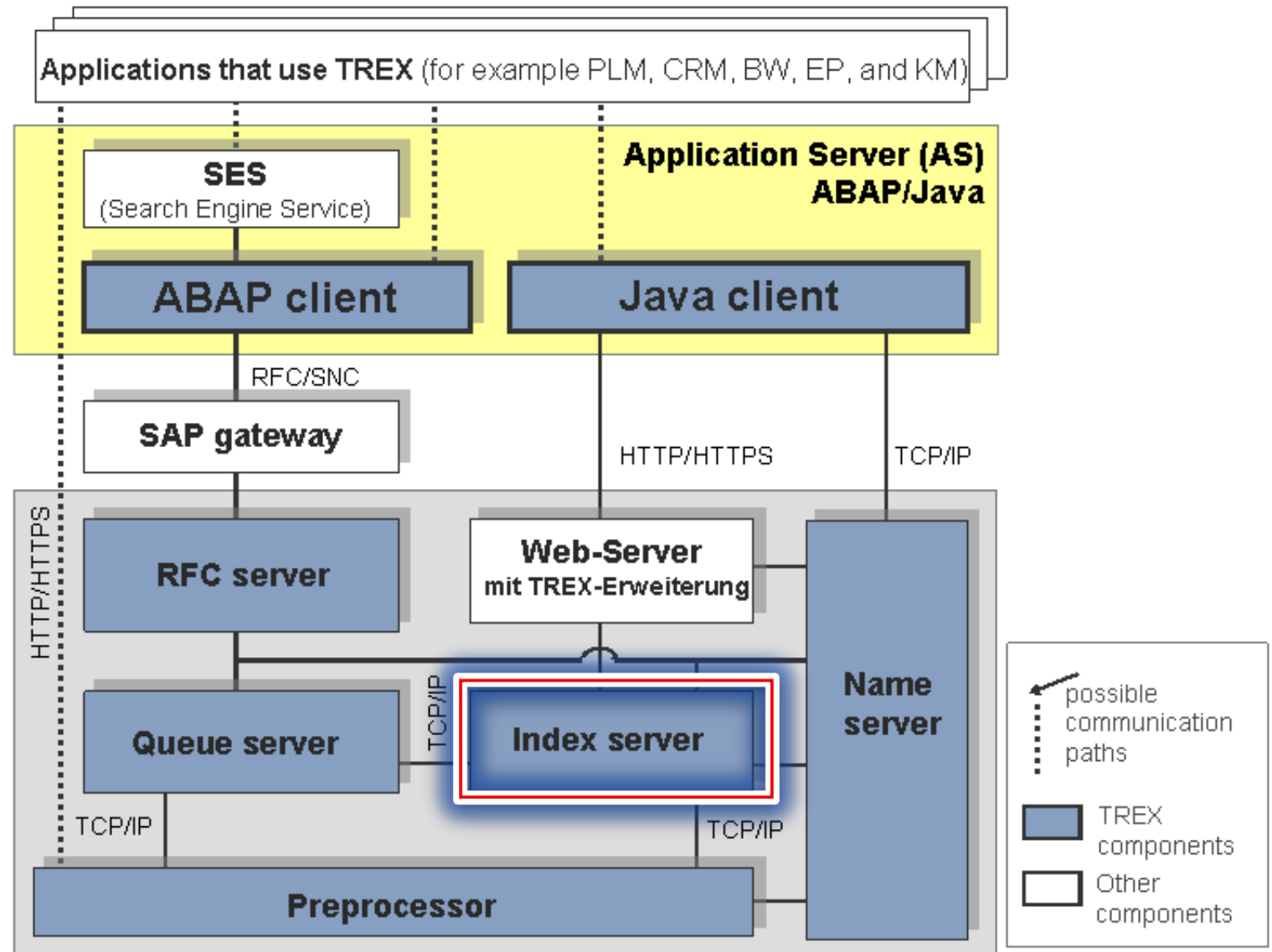
## □ Name server

- Manages topology information
- Coordinates replication services
- Load-balancing
- Ensures high availability



## Index server

- Search Engine
- Text-mining Engine
- Attribute Engine

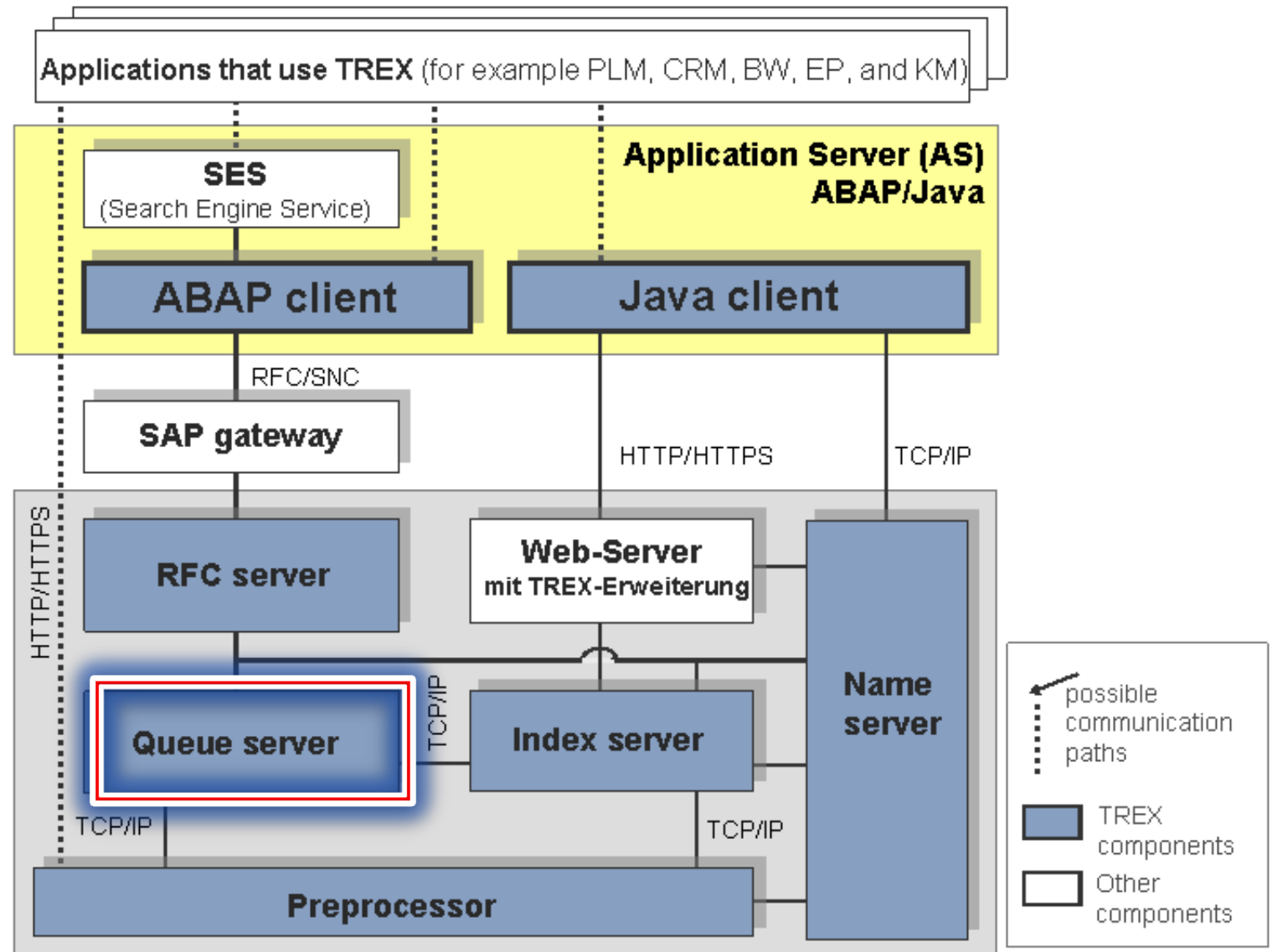


# SAP TREX | Architecture



## Queue server

- Coordinates processing steps
- Enables asynchronous indexing
- Triggers index replication and integration



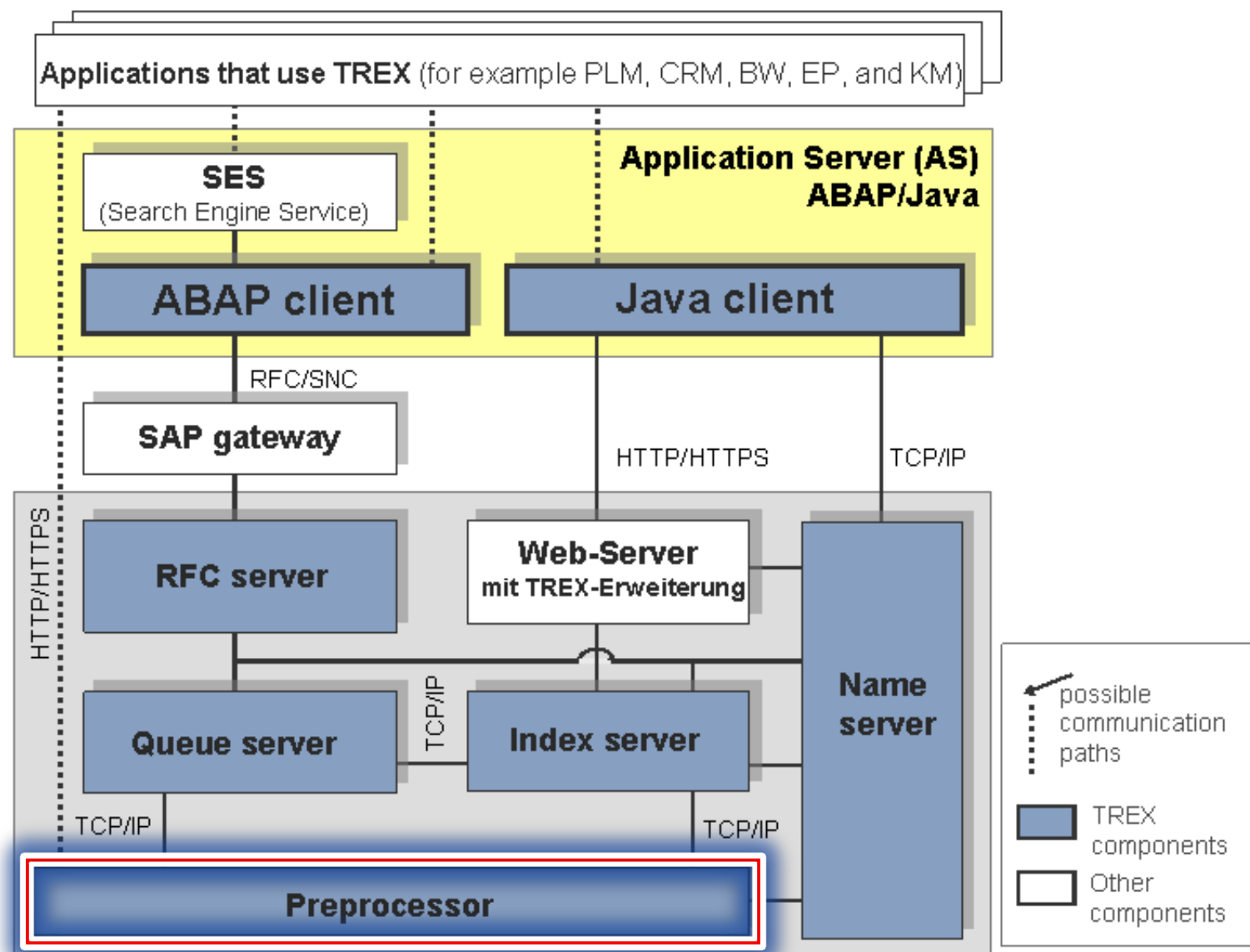


# SAP TREX | Architecture



## Preprocessor

- Retrieves documents
- Loads documents
- Filters documents
- Analyze documents linguistically

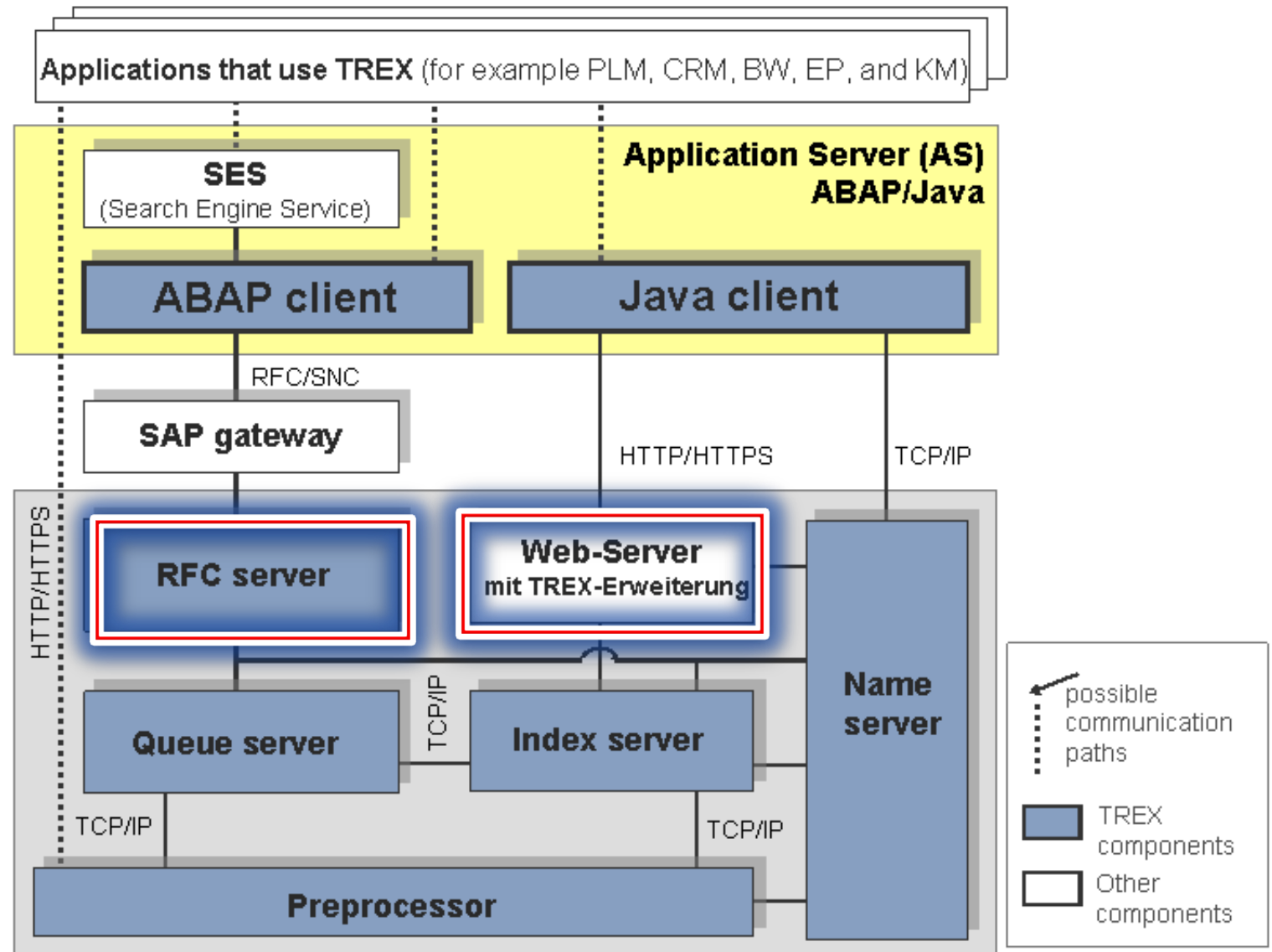


## ❑ RFC server

- Responsible for communication between SAP Systems and TREX servers
- It handles RFC requests between SAP System gateway and TREX servers

## ❑ Web server

- Responsible for communication between Java Applications and TREX servers
- It handles HTTP/HTTPS requests in XML format



# SAP TREX | Architecture



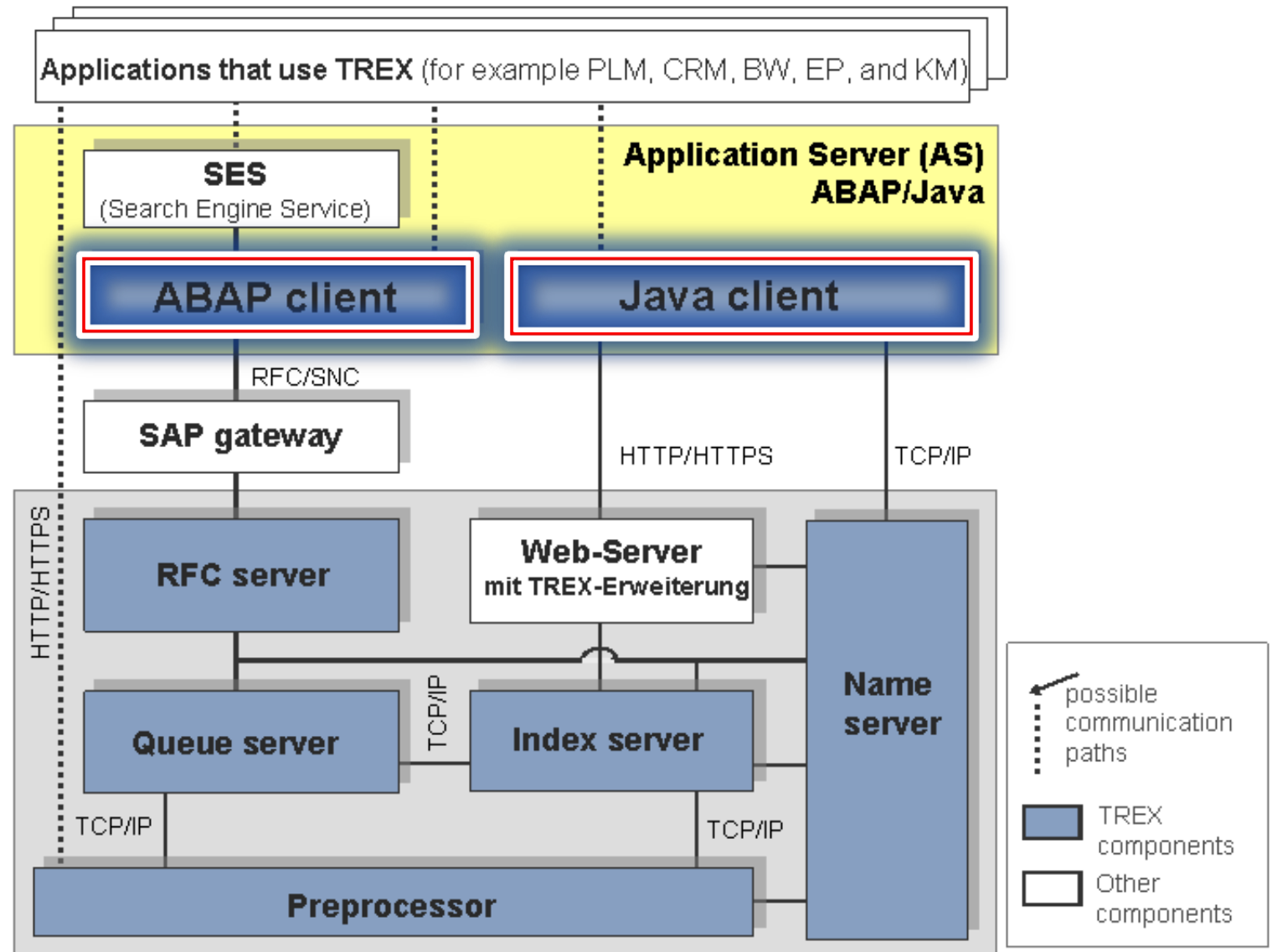
## What are we going to use?

- ☐ ABAP Client
- ☐ Java Client

“TREX APIs may only be used SAP-internally. Cannot directly be used by customers or partners”

## But...

- ☐ What if we use the same APIs that are being used by the SAP System?
- ☐ What if the SAP Gateway is not secured?
- ☐ Can we access to these APIs externally?



# Attack Scenarios


# SAP TREX | Discovery



❑ Execute nmap: `nmap -vvv -Pn -p1-65535 192.168.0.201`

```
30501/tcp open unknown
30502/tcp open unknown
30503/tcp open unknown
30504/tcp open unknown
30505/tcp open unknown
30507/tcp open unknown
30508/tcp open unknown
30511/tcp open unknown
30516/tcp open unknown
50013/tcp open unknown
50113/tcp open unknown
50513/tcp open unknown
59804/tcp open unknown
59813/tcp open unknown
64999/tcp open unknown
65000/tcp open unknown

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.94 seconds
```



**TREX Ports pattern: 3<INST><SRV>**

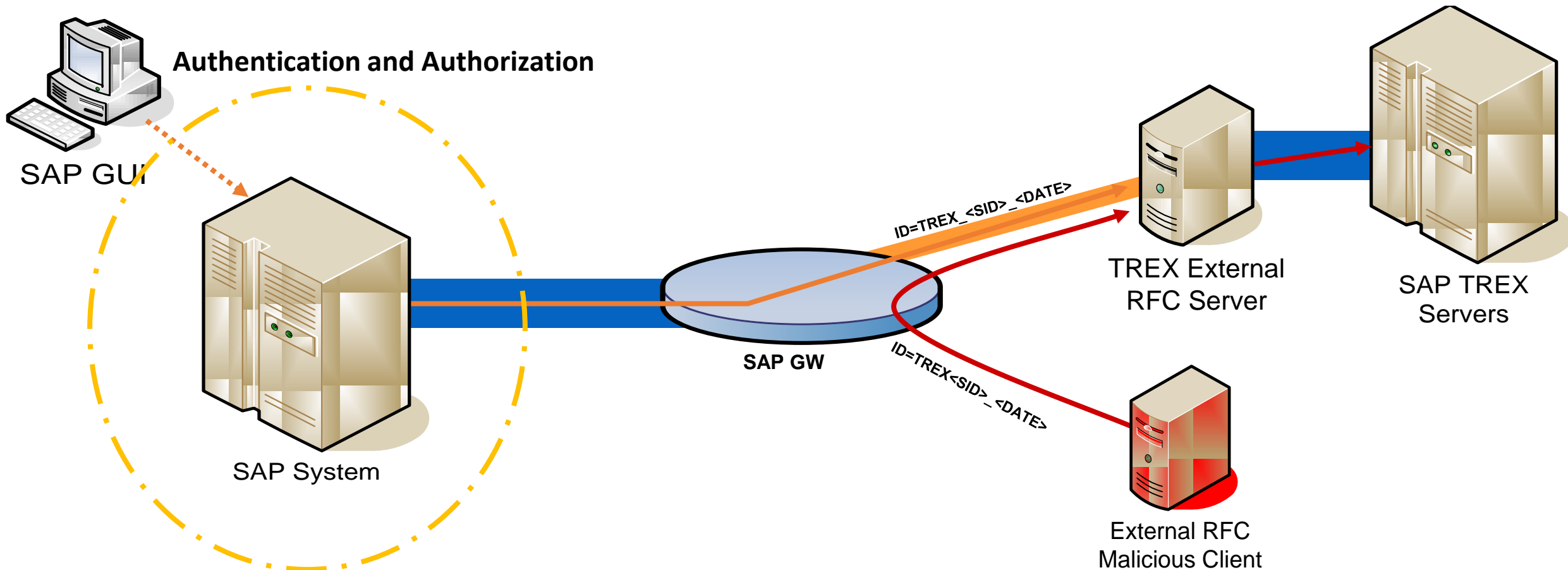
Clearly... Instance Number = 05

- ❑ Name server: 30501
- ❑ Preprocessor: 30502
- ❑ Index server: 30503
- ❑ Queue server: 30504
- ❑ HTTP server: 30505
- ❑ RFC server: 30507
- ❑ Alert server: 30508

# SAP TREX | Information Gathering (RFC)



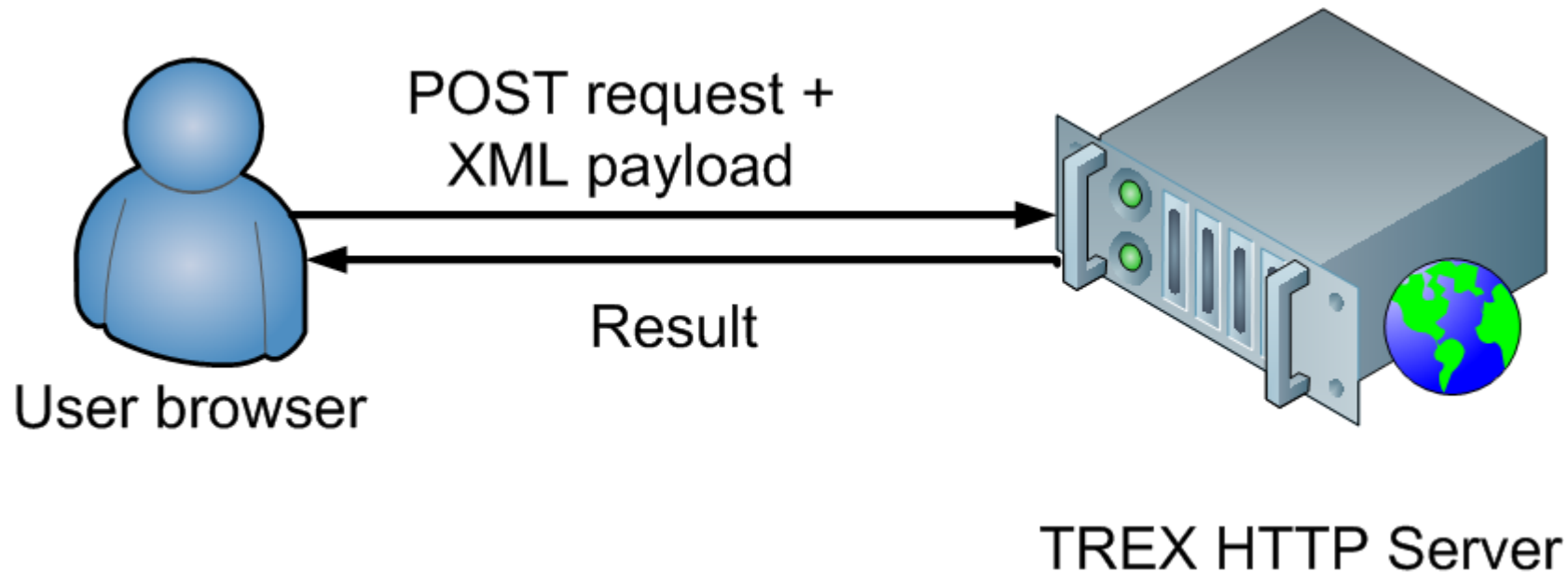
## How to connect to the TREX External RFC Server (RFC API)





# SAP TREX | Information Gathering (HTTP) onapsis

## How to connect to the TREX HTTP Server (JAVA API)



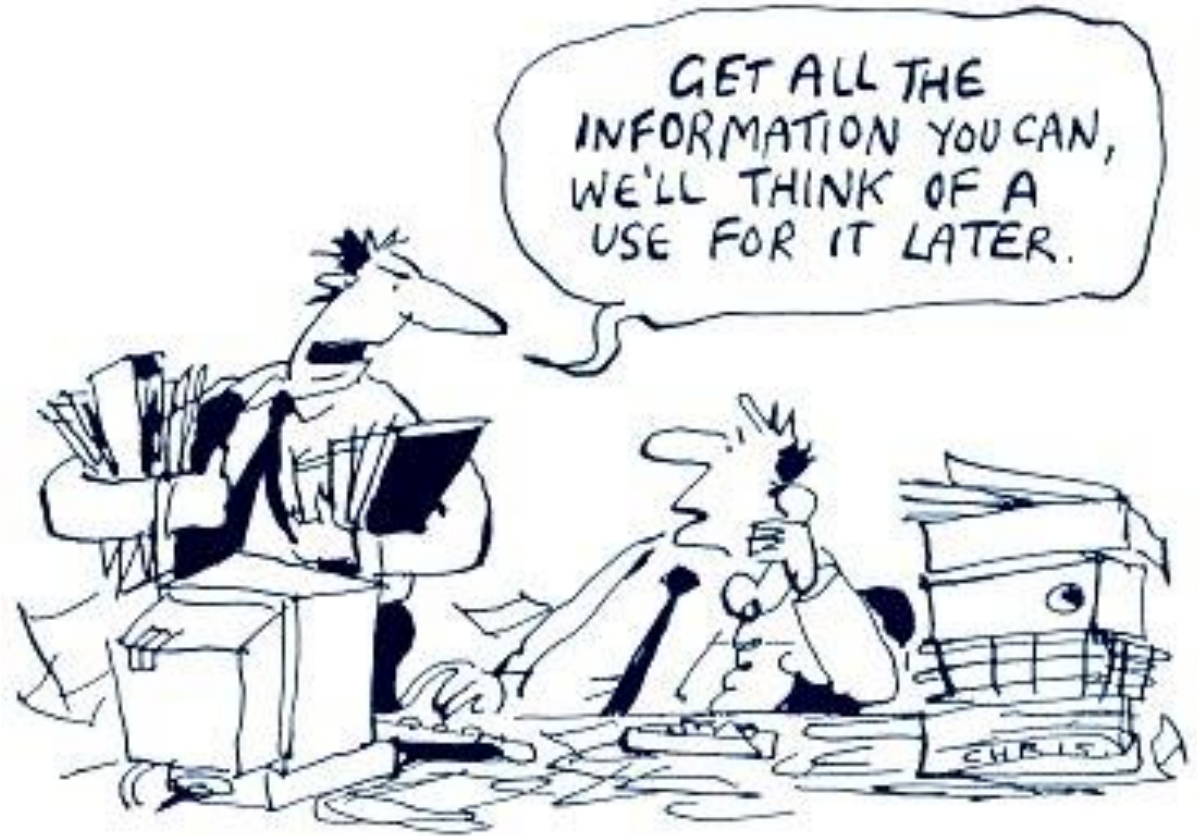
# SAP TREX | Information Gathering Demos onapsis

## ❑ Java Client

- Getting **TREX** server version
- Getting **indexes** file system path
- Getting **all** indexes

## ❑ ABAP Client

- Recognizing **TREX** Services
- Getting **ALERT** server configuration
- Getting **technical information** about **all** indexes



# Technical Information Gathering Demos

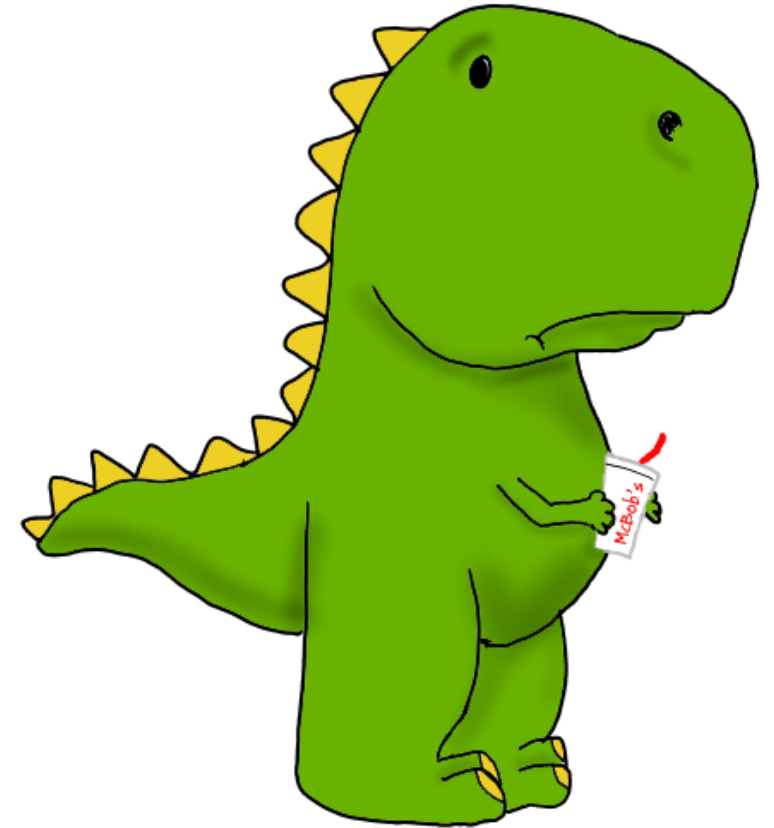
## What to do with all the information gathered?

- Now we have much more information about the technical details of TREX:
  - Having listed all indexes, choose one.
  - Extract all the technical information about that index, such as its field attributes.
  - Perform a search and get the same business information as being the SAP System, but without all the requirements.



- ❑ On the SAP Systems (i.e. the Business Suite) we have:
  - Users (authentication)
  - Access Control (Authorizations to access the information)
  - SoD checks (verify that only the employees that should perform certain tasks cannot perform incompatible tasks).
  - Strong policies, compliance checks and controls of the systems.

So why would an attacker bother to bypass all these protections, if the information is available without authentication???



# Business Information Gathering Demos

### ***Protections/ Countermeasures***



- Secure access to external servers using SAP Gateway (gw/reg\_info and other related parameters).
- Implement SNC to secure the communications with the Gateway
- Use SSL/TLS to secure the communications with the HTTP Server.
- Filter the access to TREX HTTP Server and ALL TREX Services
- Keep TREX updated to the latest version.
- *Check the “References” slide for more information!*

- Several SAP products use SAP TREX as a **backend search engine** and most of the times we are not aware of that.
- These standalone engines could potentially hold **sensitive business information** indexed from the SAP systems
- By default, there is **no authentication or encryption** protecting access to SAP TREX.
- In order to protect our business information, we need to protect **ALL** the systems and products within the landscape.
- SAP TREX is a great search and text-mining solution, but we need to understand how to protect it and the **risks** implied if we don't.
- It's not **just “a technical system”**, in fact, **everyone** could potentially access business information if it is not properly protected.



- <http://scn.sap.com/docs/DOC-8489>
- <http://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/00de20e1-6160-2b10-b6ab-dedb9d10b8e8?QuickLink=index&overridelayout=true&32461362823501>
- [https://help.sap.com/saphelp\\_nw70ehp1/helpdata/en/47/1b074063616446e10000000a114a6b/frameset.htm](https://help.sap.com/saphelp_nw70ehp1/helpdata/en/47/1b074063616446e10000000a114a6b/frameset.htm)
- <http://scn.sap.com/docs/DOC-7922>
- [http://help.sap.com/saphelp\\_nw70ehp1/helpdata/en/27/08ef417fc65f24e10000000a1550b0/frameaset.htm](http://help.sap.com/saphelp_nw70ehp1/helpdata/en/27/08ef417fc65f24e10000000a1550b0/frameaset.htm)
- [https://help.sap.com/saphelp\\_nwes73/helpdata/en/4a/436c97edf31c62e10000000a42189c/frameset.htm](https://help.sap.com/saphelp_nwes73/helpdata/en/4a/436c97edf31c62e10000000a42189c/frameset.htm)
- <http://scn.sap.com/docs/DOC-8466>



## Questions?

Juan Perez-Etchegoyen  
[jppereze@onapsis.com](mailto:jppereze@onapsis.com)  
[@jp\\_pereze](https://twitter.com/jp_pereze)

Sergio Abraham  
[sabraham@onapsis.com](mailto:sabraham@onapsis.com)  
[@serj\\_ab](https://twitter.com/serj_ab)



onapsis

