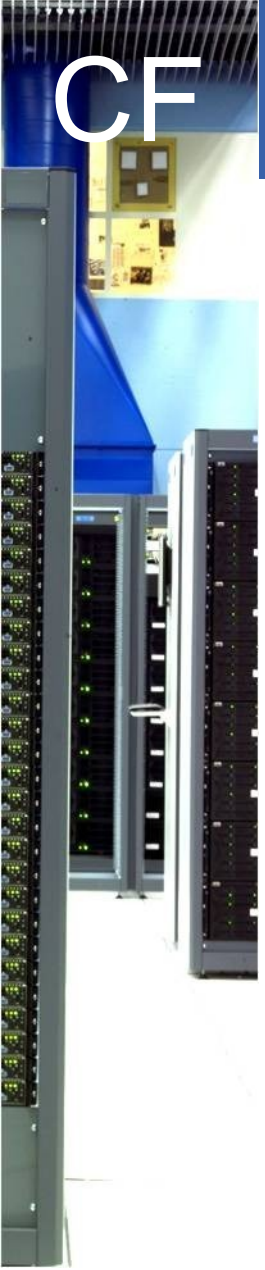
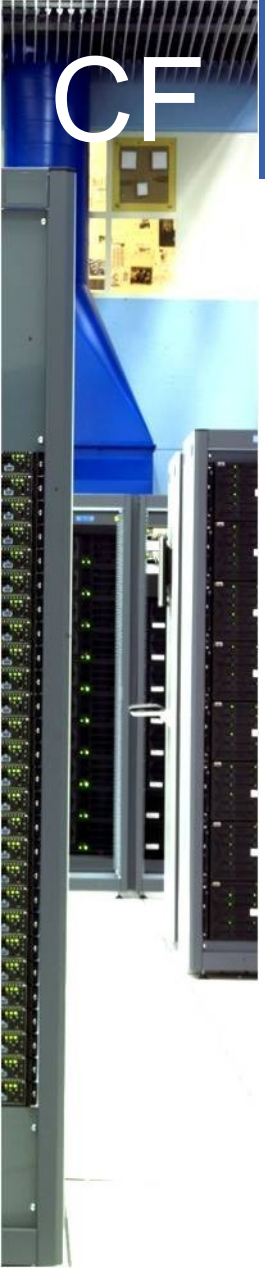


SINDES v1 & v2

Secure INformation DElivery System

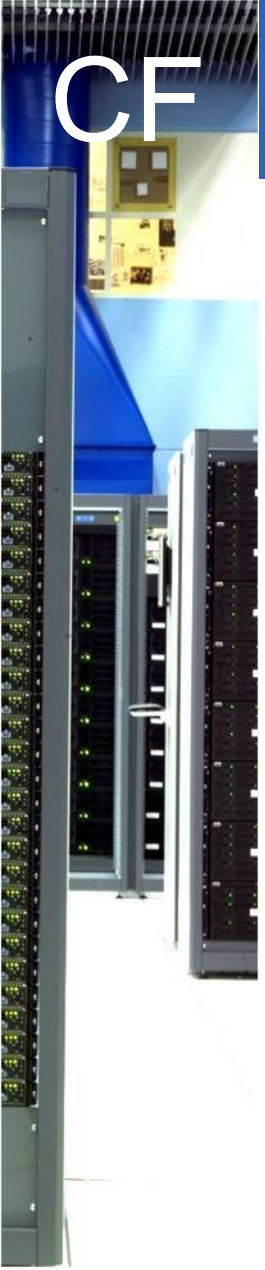
CERN IT/CF-ASI

CERN IT
Department
CH-1211 Geneva
23
Switzerland



Outline

- **What is SINDES v1**
- Weak points of SINDES v1
- Requirements and opportunities
- SINDES v2 overview
- What will change
- Prove of the concept
- SINDES v2 Architecture



What is SINDES

CERN IT Department

Main purpose of SINDES:

- CA - manage the certificates

1. providing interface for (re)installation process,
2. node/user authentication and authorization,

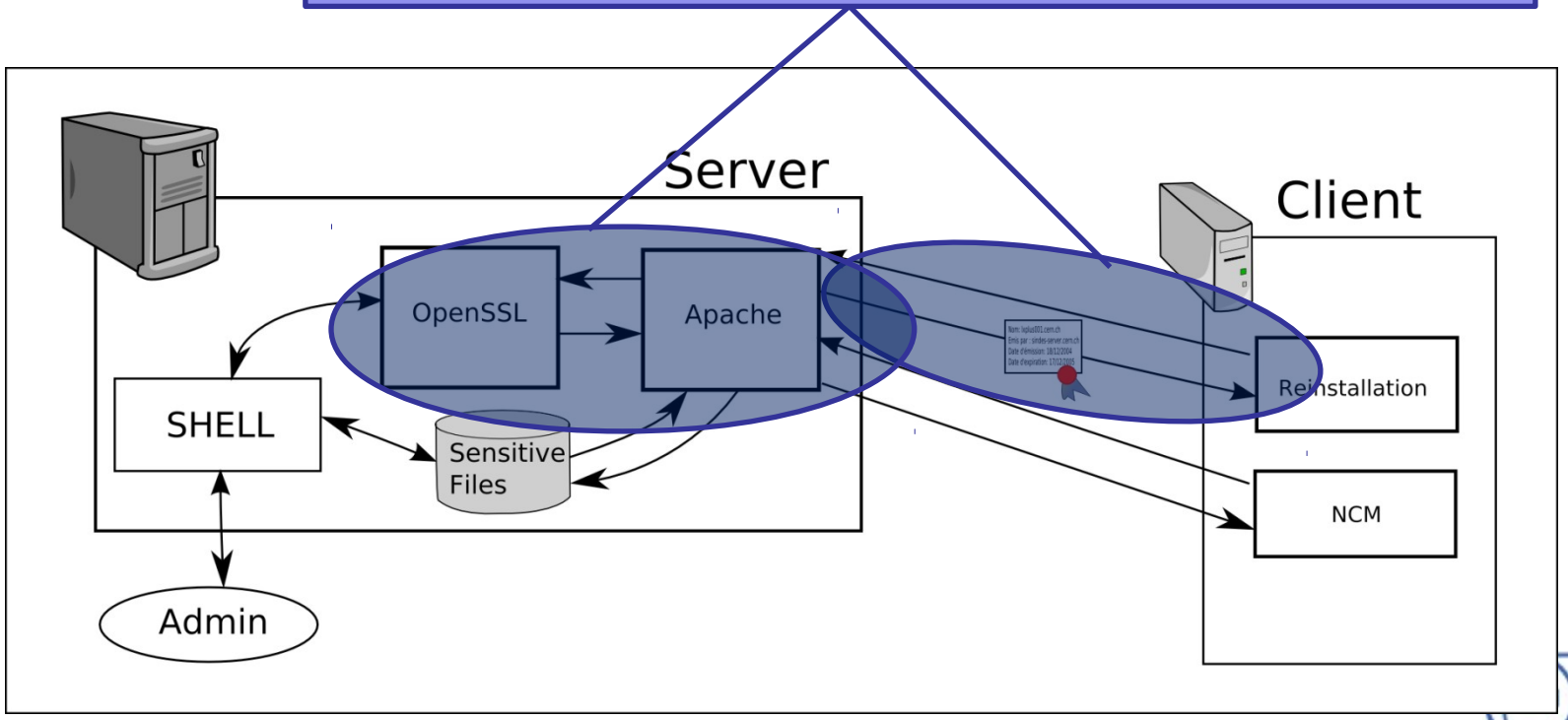
- Store & deliver confidential information

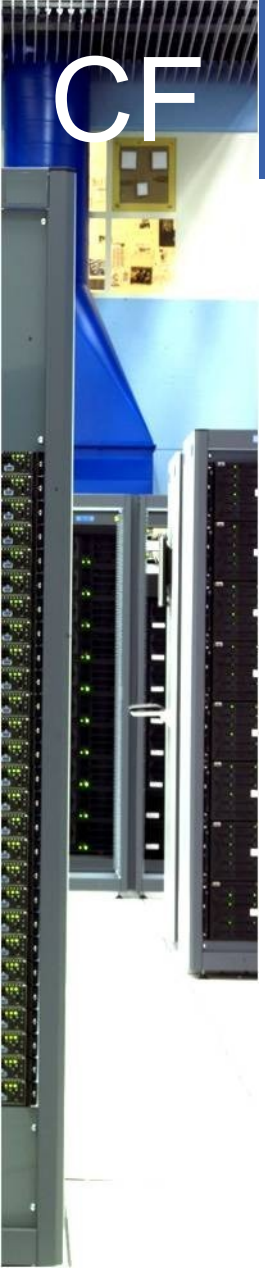
1. secure data (file) storage,
2. secure bidirectional file transfer between SINDES server and host/user,
3. keeping consistency with CDB configuration of the host.

SINDES – Certificate Authority

CA functionality:

- Create certificates
- Sign certificates
- Confirm identities
- Revoke certificates



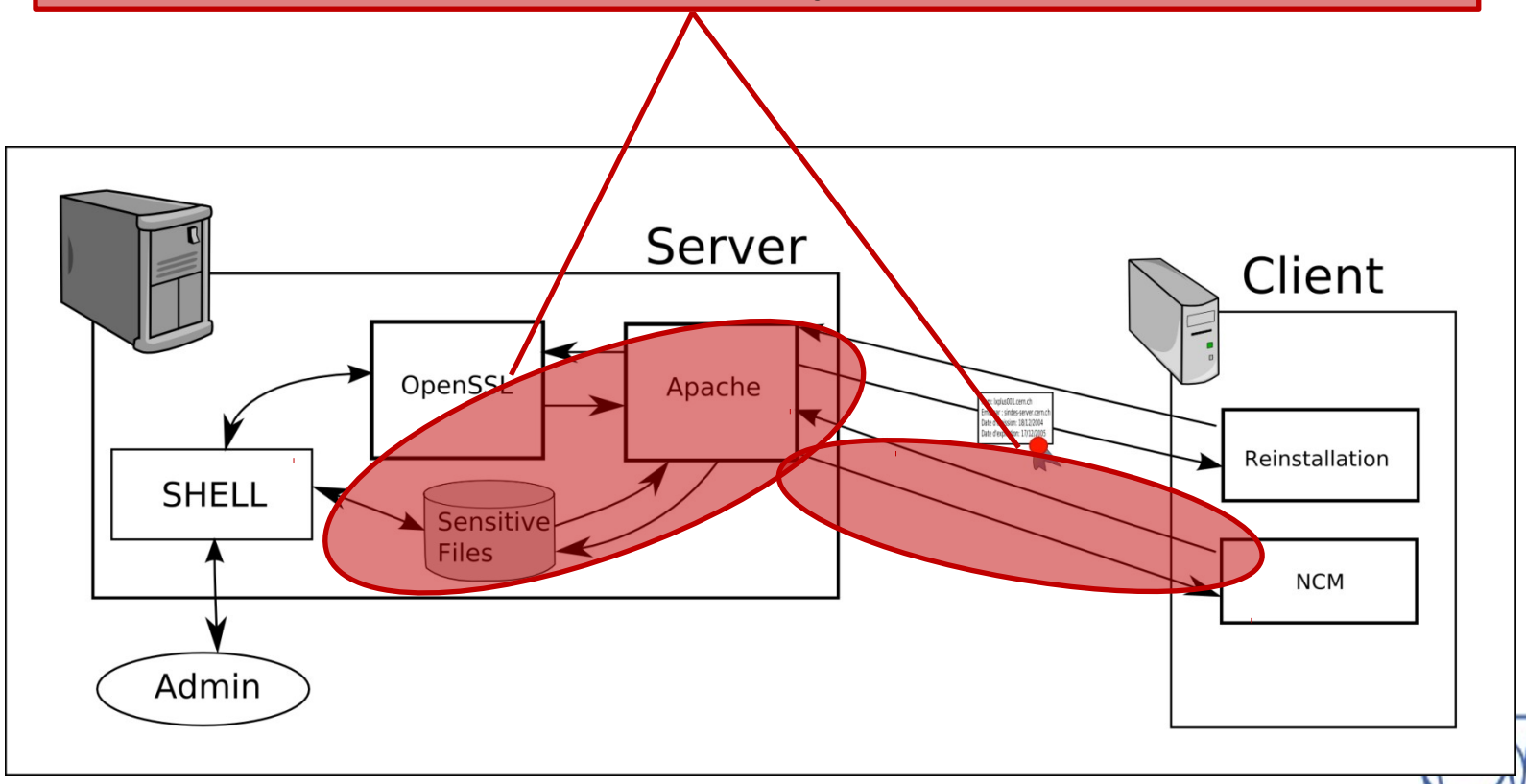


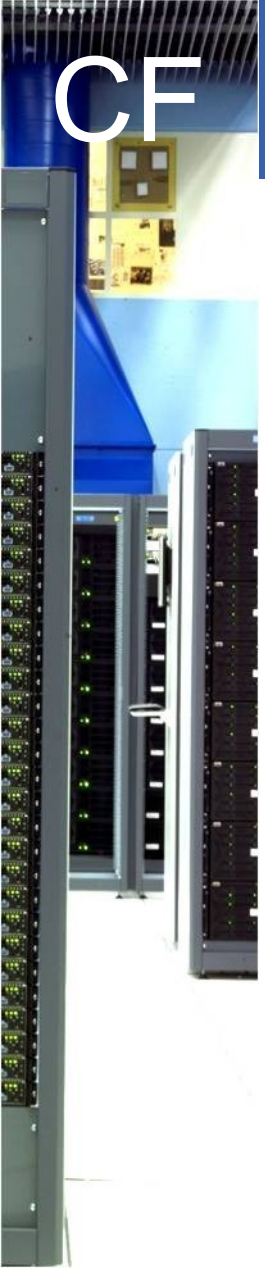
SINDES – Storage & delivery

CERN IT Department

Storage centre

- Upload secret files
- Store passwords
- Deliver files in a secure way





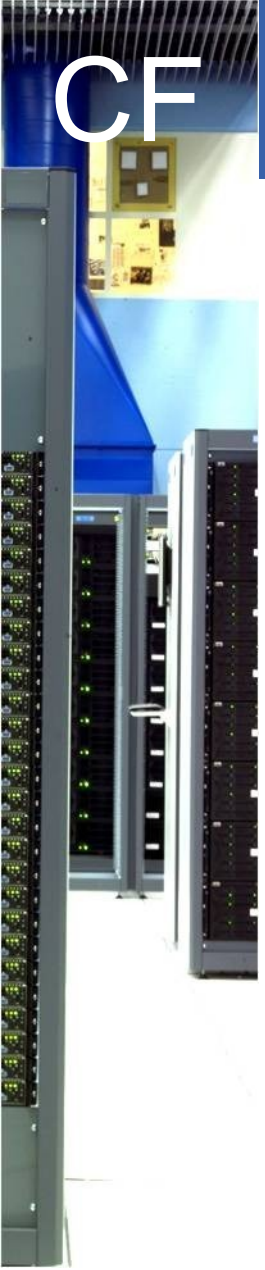
What is SINDES

CERN IT Department

- **Main purpose:**
  - CA - manage the certificates
  - Store & deliver confidential information

- **Architecture** based on OpenSSL x509 standard, Apache with mod_ssl and mod_rewrite

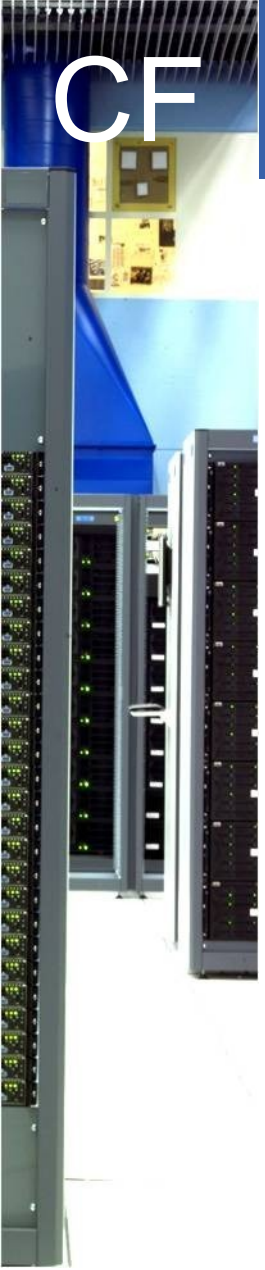
- **Automated** certification process – client has defined time window to ask for a certificate



Outline

- What is SINDES v1
- **Weak points of SINDES v1**
- Requirements and opportunities
- SINDES v2 overview
- What will change
- Prove of the concept
- SINDES v2 Architecture

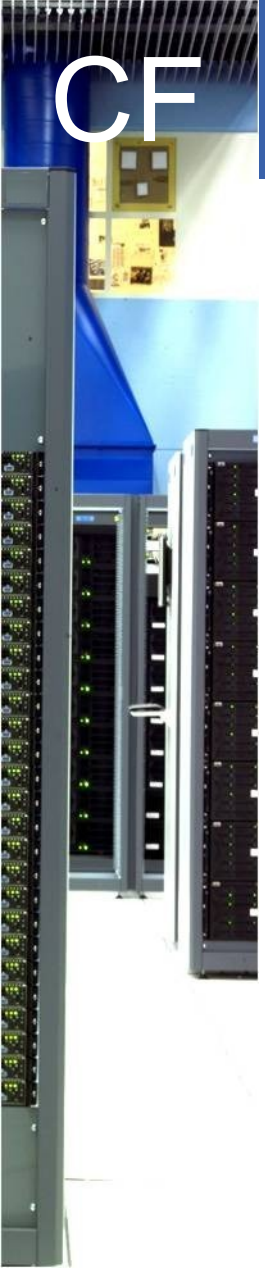
Weak points of SINDES



Usability

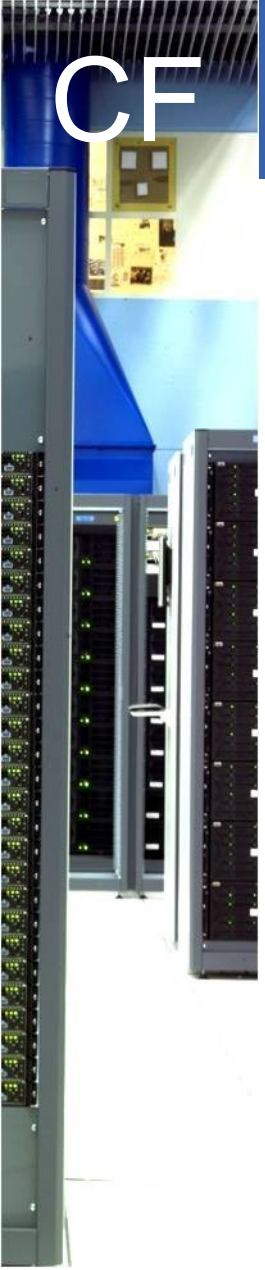
- No delete file feature
- Only two target types (structure limitation):
  - cluster
  - host
  - today also subcluster type needed
- No mechanism to move a machine between clusters
- No view file feature; fetch file to client only
- No file versioning

Weak points of SINDES



Security issues:

- Only one SINDES system user
  - anybody with the access may tamper any file stored with SIDNES
  - no user information in log files
- No privileges granularity
  - you have access to SINDES = you can modify every item inside



Weak points of SINDES

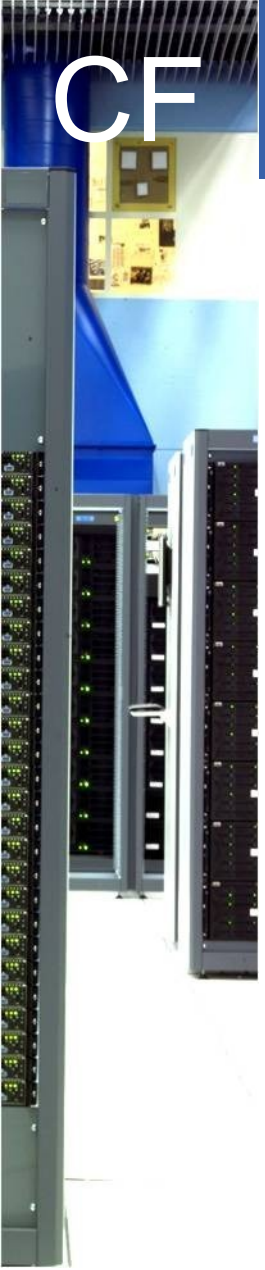
On the one hand:

- System in production serving more than 8.000 hosts at CERN

- A number of crucial applications relying on SINDES CA functionality to authenticate (i.e. Lemon, CDB, CluMan)

On the other hand:

- Limited functionality
- Room for improvement in security aspect



How to improve SINDES

CERN IT Department

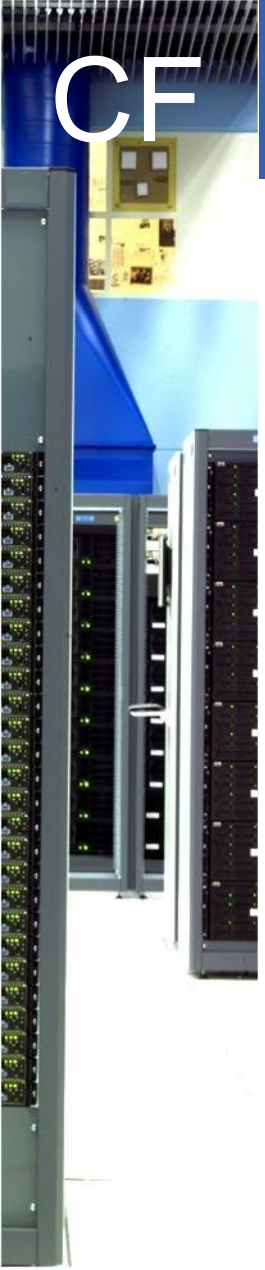
Ways of improvement – from October 2010

- Enhance the usability and security in the current version of the system

- Find and adopt a new tool, keep the functionality
  Freeware tools: i.e. *wallet* by Russ Allbery
  http://www.eyrie.org/~eagle/software/wallet/

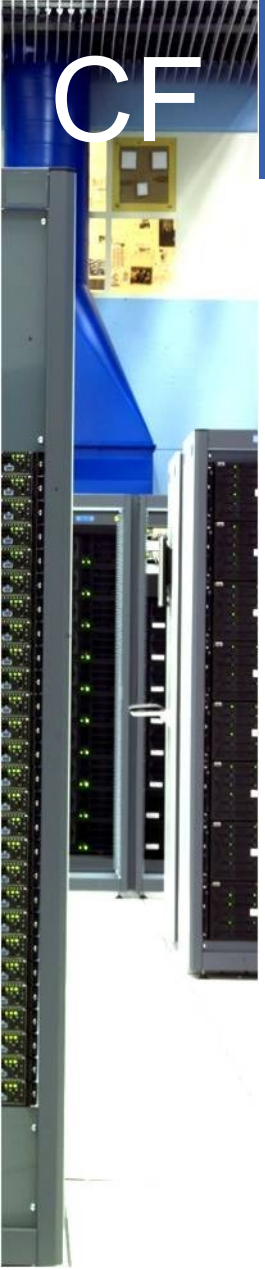
- Write a completely new tool

We have 1 year manpower starting from the 1st October 2010



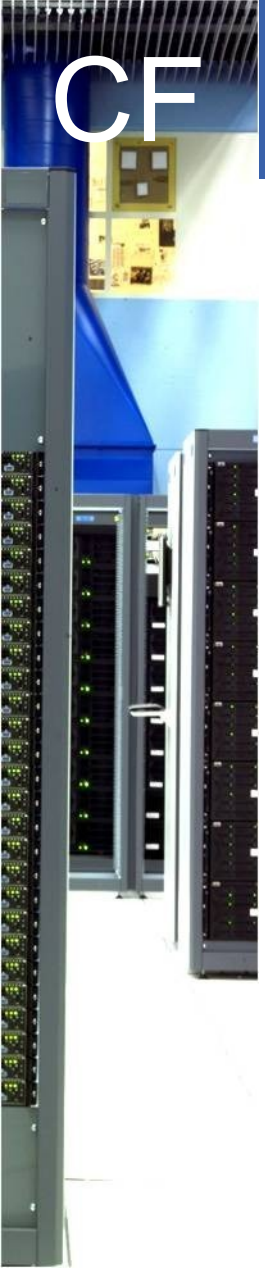
Progress since Oct 2010

- SINDES wiki moving to Quattor website
- Trying to publish SINDES on sourceforge on Apache2 license
- Development:
  - Some minor bugs fixed
  - Access control based on CDB and LanDB implemented
  - Enhanced logging



Outline

- What is SINDES v1
- Weak points of SINDES v1
- **Requirements and opportunities**
- SINDES v2 overview
- What will change
- Prove of the concept
- SINDES v2 Architecture



SINDES Requirements

CERN IT Department

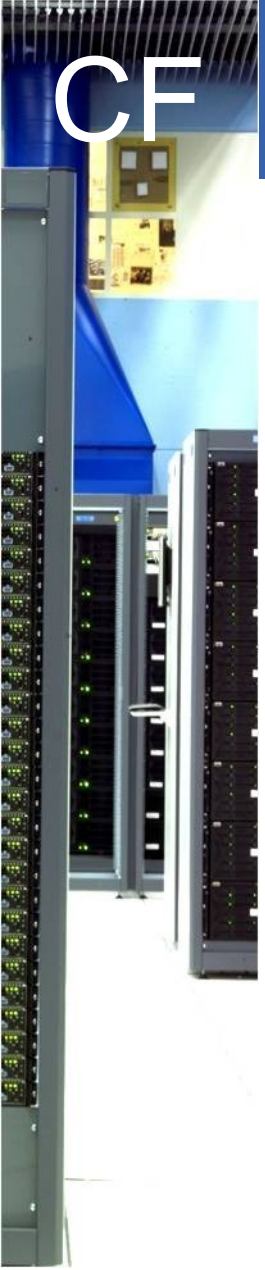
Requirements from CERN users collected

File storage:

- User may view, download, modify and delete a file from SINDES
- Add file versioning feature
- Allow machine to upload items back to SINDES

Structure:

- Support host move from one cluster to another
- Support subclusters
- Support namespaces in clusers/hosts



SINDES Requirements

CERN IT Department

Security:

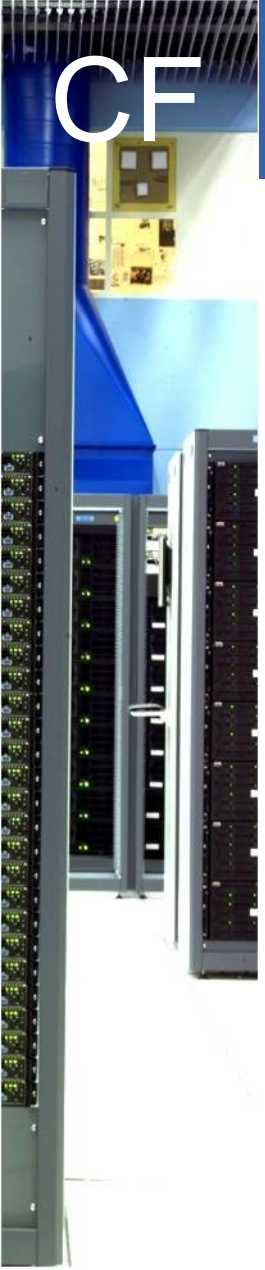
- Restrict users to modify only files related to their host/items
- Unattended installation - allow a node to access the certificate/private key without opened time window

Scripts:

- Passwd.header support different OS

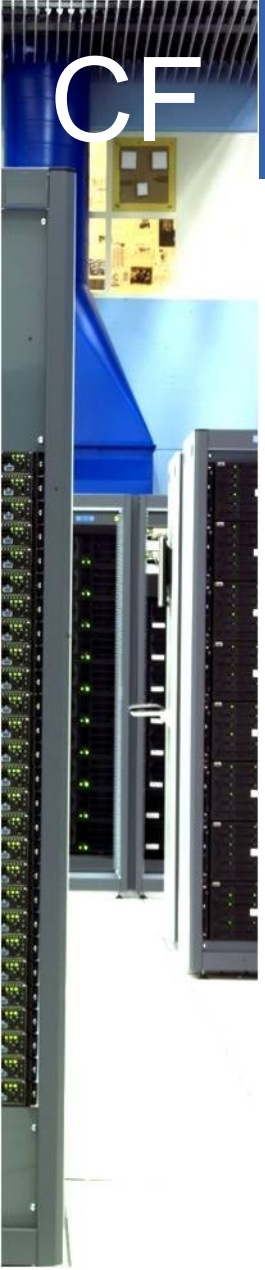
Architecture & security:

- Review the security at all the levels
- Review the architecture of SINDES
- Separate SINDES CA from file storage functionality
- Enhance documentation



Outline

- What is SINDES v1
- Weak points of SINDES v1
- Requirements and opportunities
- **SINDES v2 overview**
- What will change
- Prove of the concept
- SINDES v2 Architecture



SINDES v2 overview - goals

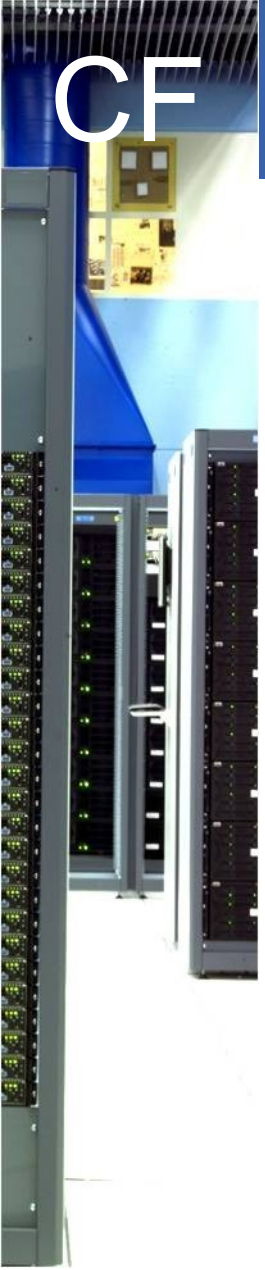
CERN IT Department

1. Simplicity:
   - use external services whenever possible
   - easy to maintain

2. Flexibility
   - provide flexible structure of files

3. Implement new requests and keep current functionality

CERN



SINDES v2 overview

CERN IT Department

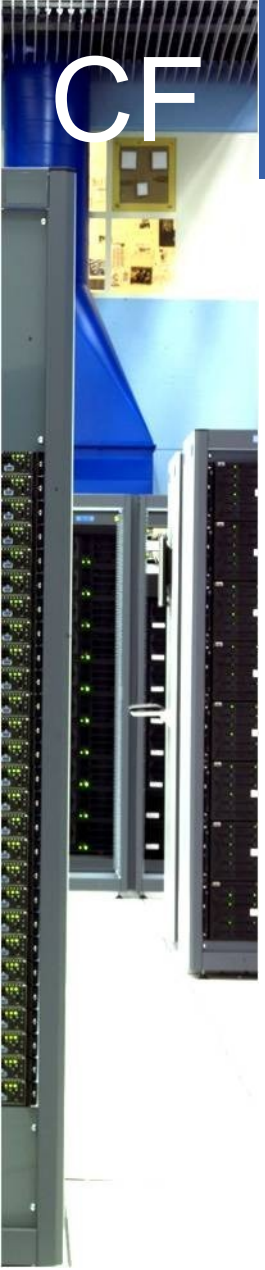
SINDES2 server consists of:

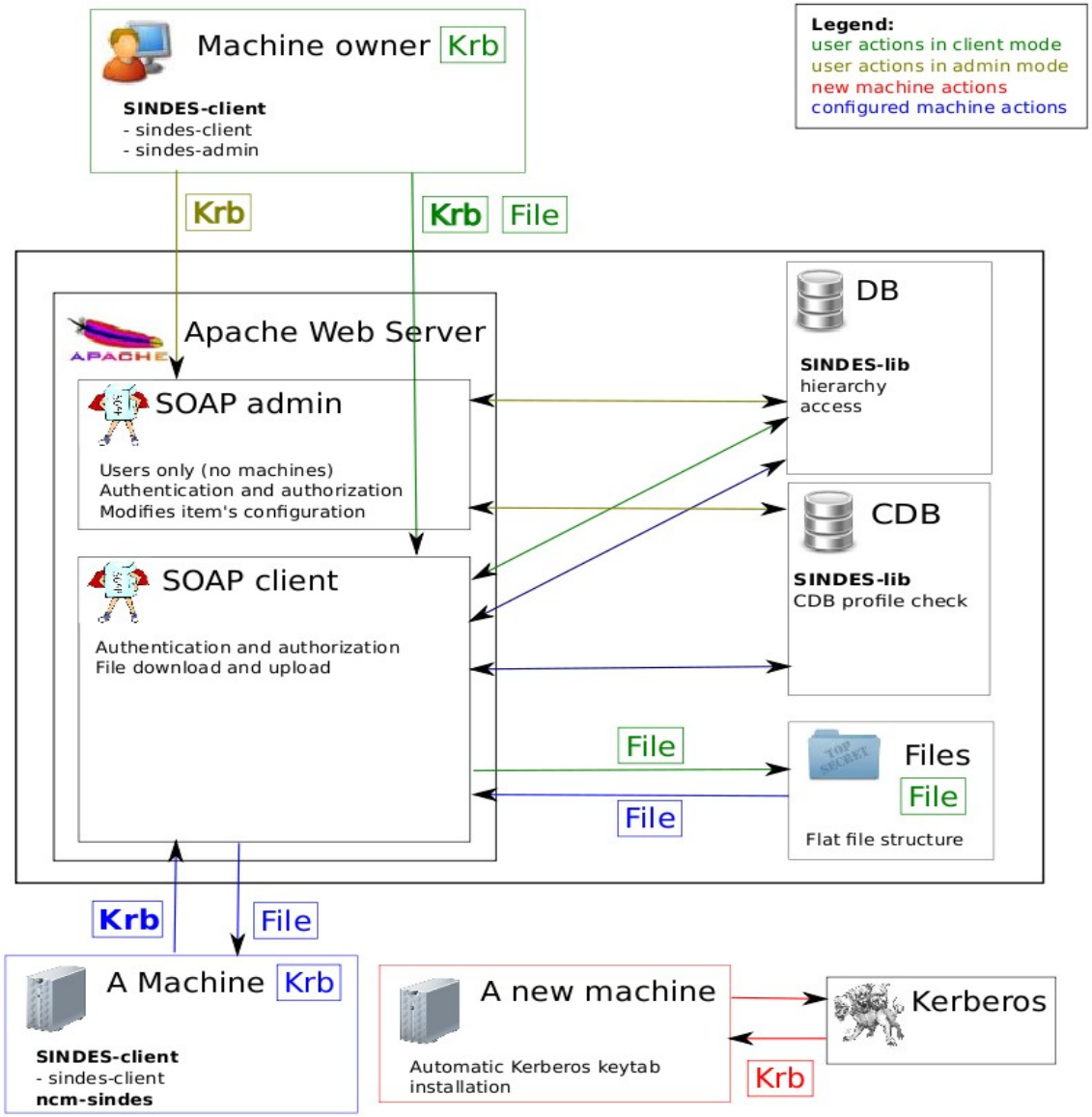
- Apache web server with SOAP services,
- authentication and authorization module,
- SINDES2 configuration database module,
- CERN CDBSQL query module
- item's directory with SVN in the background.

- sindes-client script,
  - same for user and node
  - for uploading and downloading
  - one entry point on server side
- sindes-admin script for managing access, etc.

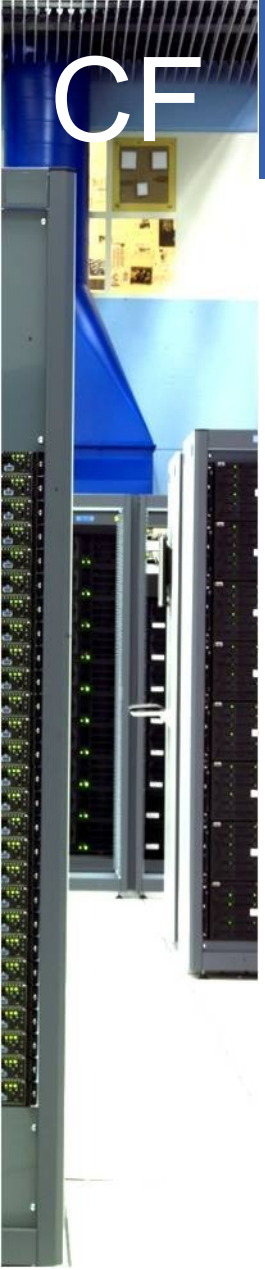
- KRB authentication instead if certificates
- A number of services behind

SINDES v2 overview





CERN IT
Department
CH-1211 Geneva
23
Switzerland

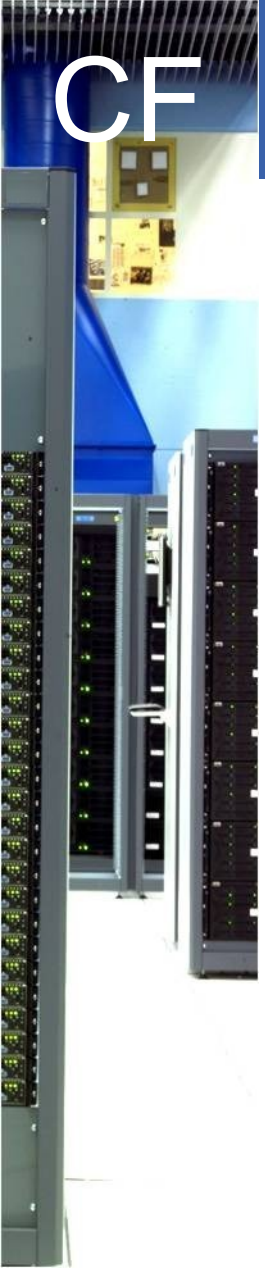


What will change?

CERN IT Department

- No SINDES CA – Kerberos used instead
- Flexible file structure

  one may create item for selected:
  - clusters
  - subclusters
  - hosts
- Privileged user may upload/download items as he was a host
- No server-side scripts – client does the work (??)



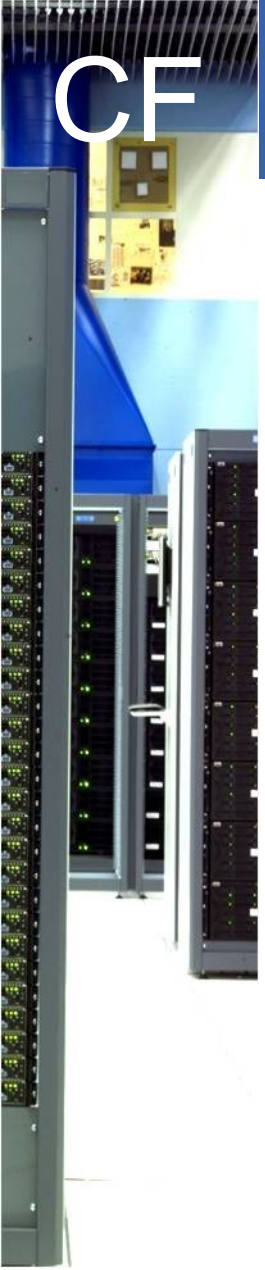
Prove of the concept

- All the core functionalities of SINDES v1 has been implemented

- All the requirements has been fulfilled:
  - Access control
  - Flexible structure (easy item move, items assigned to any node in the structure)
  - The same tools for human user and host

- Apart from that:

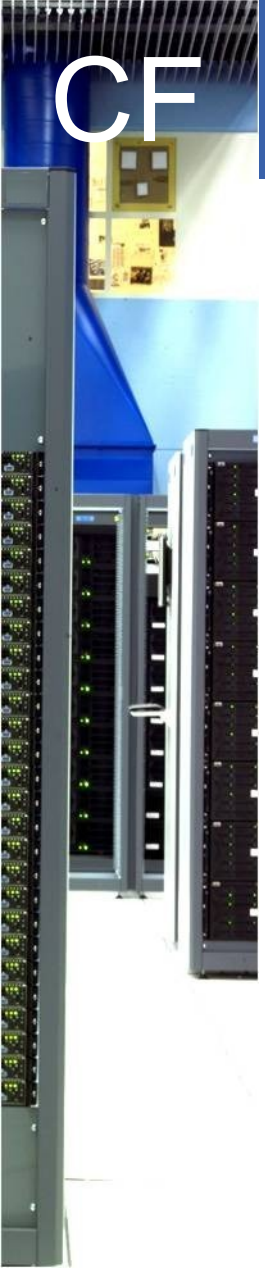
  SINDESv2 ~= 300 lines now
  SINDESv1 ~= 10.000 lines
  Less code = easier to maintain



Outline

CERN IT Department

- What is SINDES v1
- Weak points of SINDES v1
- Requirements and opportunities
- SINDES v2 overview
- What will change
- Prove of the concept
- **Example**
- SINDES v2 Architecture (poster)



Examples

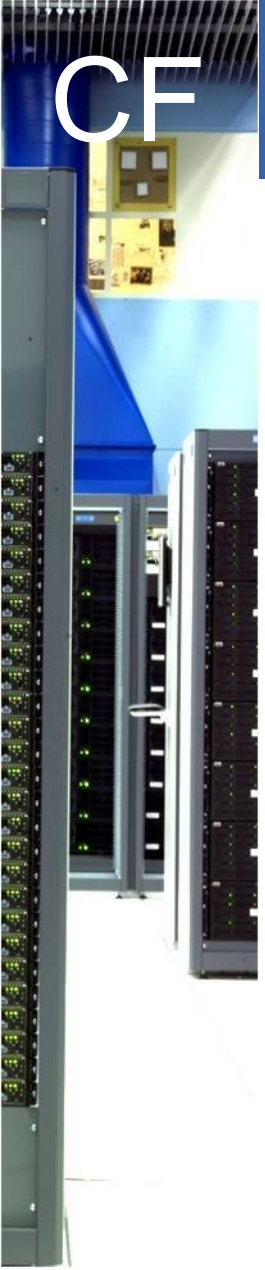
CERN IT Department

- **Upload**

```
root@sindesdev03:~# sindes-client -action upload -mode node
-item 111 -file my_item.tar.gz
SINDES2: authentiaction... node: sindesdev03
SINDES2: item 111 found
SINDES2: authorization... ok
SINDES2: file transfered
SINDES2: file saved
```

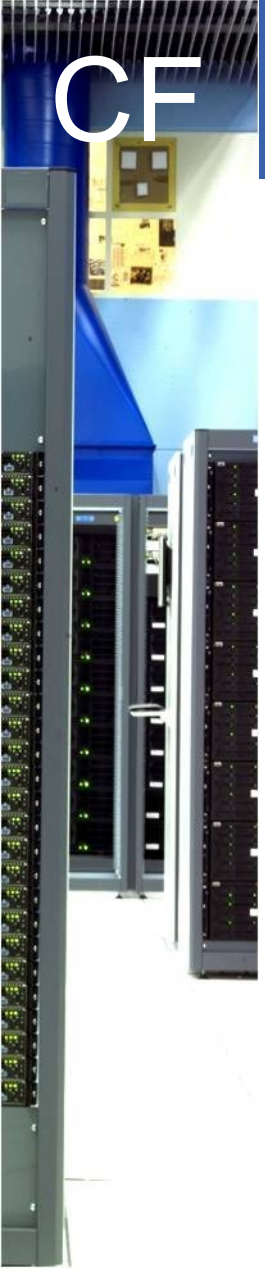
- **Download**

```
root@sindesdev03:~# sindes-client -action download -mode user
-item 111 -file my_item.tar.gz
SINDES2: authentiaction... user: jdudziec
SINDES2: item 111 found
SINDES2: authorization... ok
SINDES2: file transfered
SINDES-CLIENT: file saved
```



Outline

- What is SINDES v1
- Weak points of SINDES v1
- Requirements and opportunities
- SINDES v2 overview
- What will change
- Prove of the concept
- Example
- **SINDES v2 Architecture (poster)**



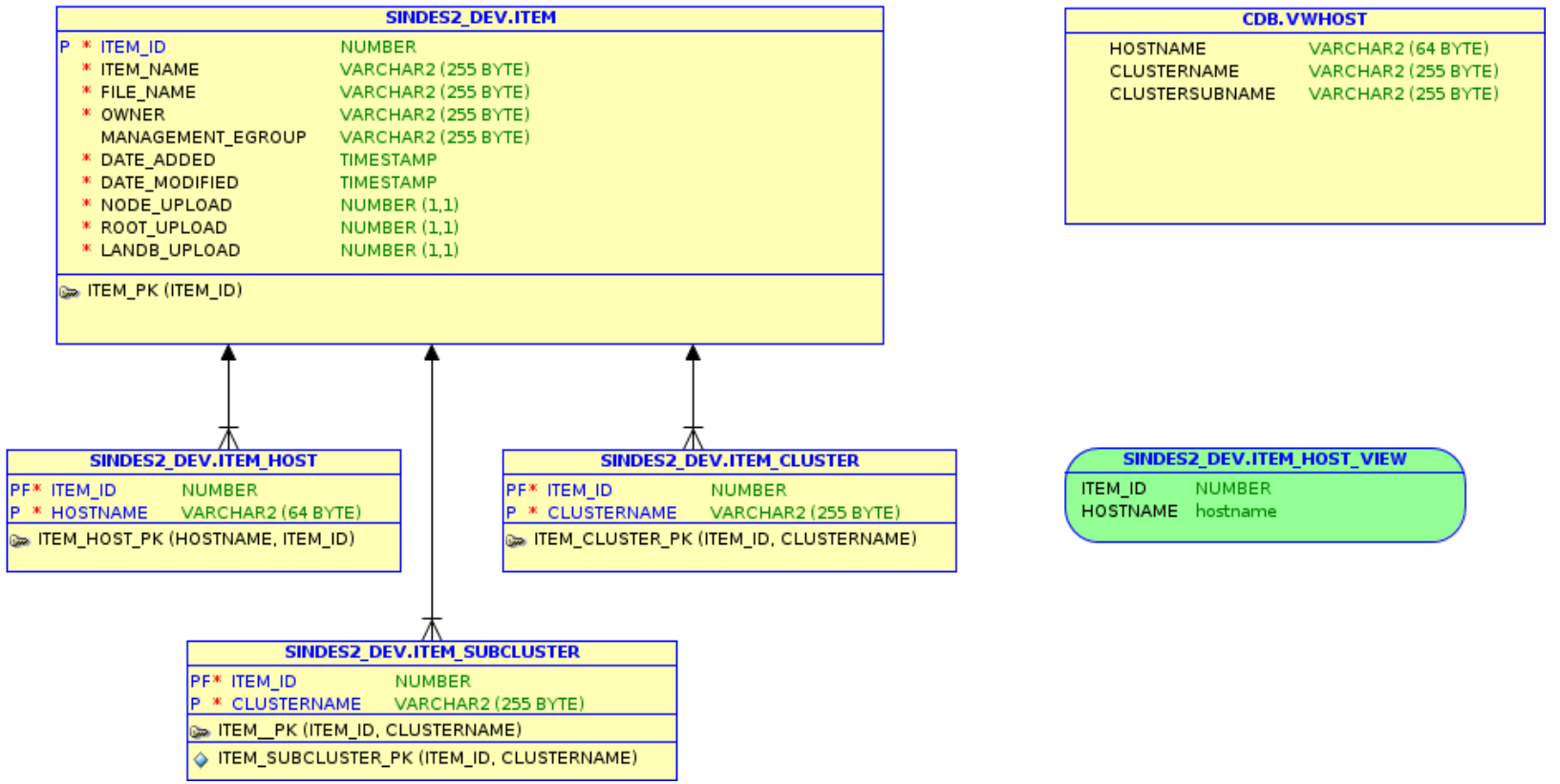
SINDESv2 Architecture

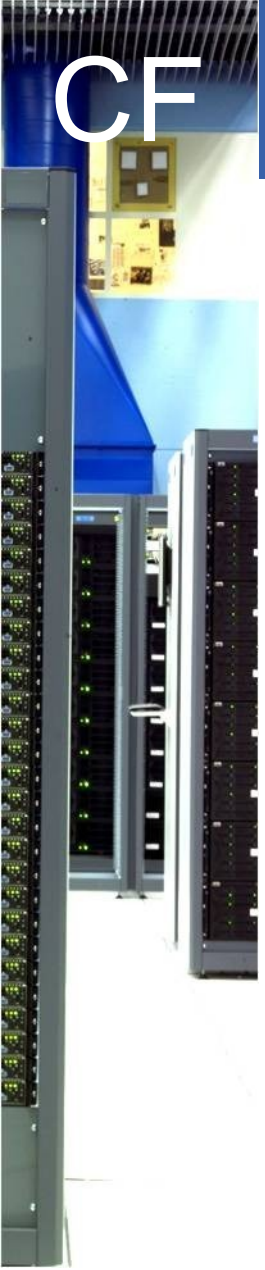
CERN IT Department

1. Components

- Server: Apache2 + mod_perl + 2 SOAP Interfaces
- SINDES2 DB
- Flat file structure
- Admin Interface (management)
- Client interface (upload/download)
- Common libraries (AuthN & AuthZ)
- Dependent services (CDB SQL, LanDB, ActiveDirectory, CDB, KRB)
- Client-side scripts

SINDESv2 DB


SINDES2_DEV.ITEM
P * ITEM_ID NUMBER
* ITEM_NAME VARCHAR2 (255 BYTE)
* FILE_NAME VARCHAR2 (255 BYTE)
* OWNER VARCHAR2 (255 BYTE)
MANAGEMENT_EGROUP VARCHAR2 (255 BYTE)
* DATE_ADDED TIMESTAMP
* DATE_MODIFIED TIMESTAMP
* NODE_UPLOAD NUMBER (1,1)
* ROOT_UPLOAD NUMBER (1,1)
* LANDB_UPLOAD NUMBER (1,1)
ITEM_PK (ITEM_ID)
CDB.VWHOST
HOSTNAME VARCHAR2 (64 BYTE)
CLUSTERNAME VARCHAR2 (255 BYTE)
CLUSTERSUBNAME VARCHAR2 (255 BYTE)
SINDES2_DEV.ITEM_HOST
PF* ITEM_ID NUMBER
P * HOSTNAME VARCHAR2 (64 BYTE)
ITEM_HOST_PK (HOSTNAME, ITEM_ID)
SINDES2_DEV.ITEM_CLUSTER
PF* ITEM_ID NUMBER
P * CLUSTERNAME VARCHAR2 (255 BYTE)
ITEM_CLUSTER_PK (ITEM_ID, CLUSTERNAME)
SINDES2_DEV.ITEM_HOST_VIEW
ITEM_ID NUMBER
HOSTNAME hostname
SINDES2_DEV.ITEM_SUBCLUSTER
PF* ITEM_ID NUMBER
P * CLUSTERNAME VARCHAR2 (255 BYTE)
ITEM__PK (ITEM_ID, CLUSTERNAME)
ITEM_SUBCLUSTER_PK (ITEM_ID, CLUSTERNAME)



SINDESv2 DB 2

SINDES2

ITEM

ID
1
2
3

ITEM_CLUSTER

ITEM	CLUSTER
1	A
2	B
3	A

ITEM_HOST

ITEM	HOST
2	A/A1
3	B/B1

CDB SQL

VW_HOSTS

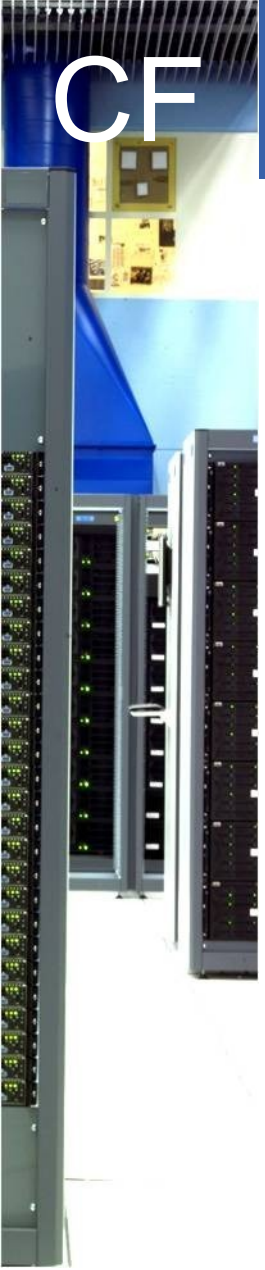
HOST	CLUSTER
A1	A
A2	A
B1	B
B2	B

ITEM_HOST_VIEW

ITEM	HOST
1	A1
1	A2
2	B1
2	B2
2	A1
3	A1
3	A2
3	B1

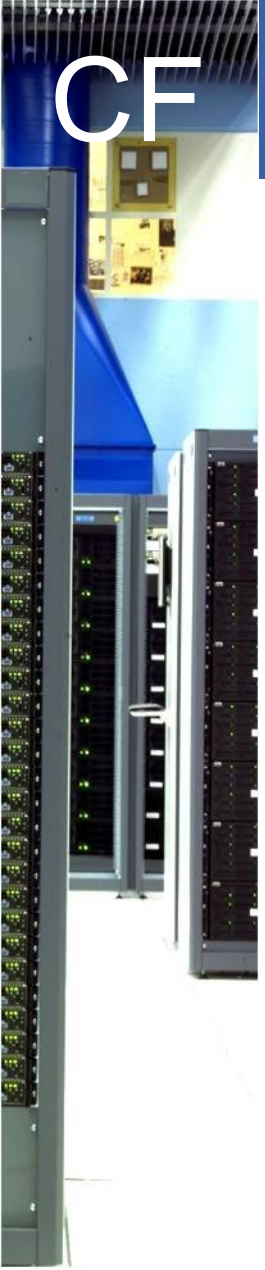
CERN IT Department
CH-1211 Geneva 23
Switzerland

SINDESv2 Architecture 2



2. Processing

- Machine (node)
  - Upload
  - Download
- Machine owner (user)
  - Upload
  - Download
  - Item management



SINDESv2 Authentication

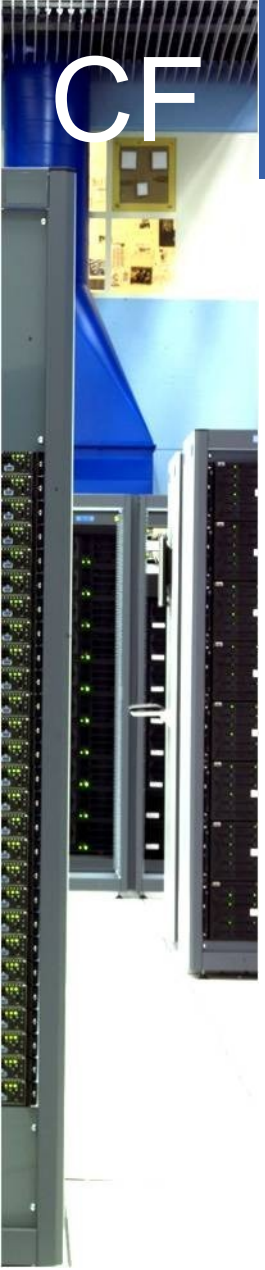
3. Authentication

Client

- Having tgt ask for ticket for SINDES2 service on sindes-server
- Send ticket

Server

- Decrypt received ticket with own keytab
- **Now we know who we are talking with**



SINDESv2 Authorization

CERN IT Department

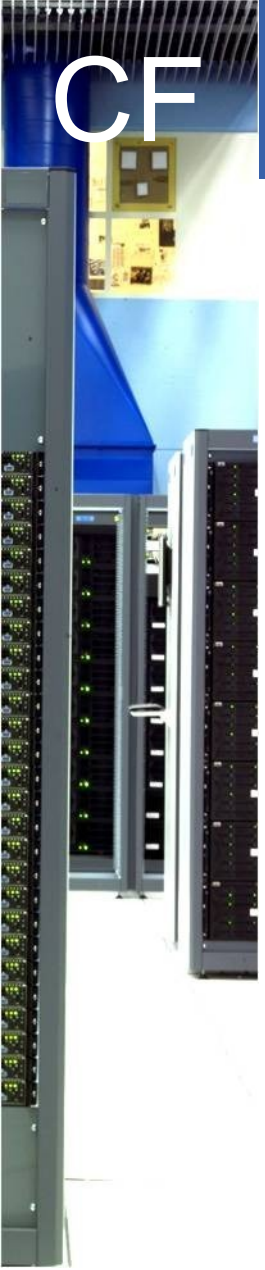
- **4. Authorization (modules)**

Node

- Download: DB lookup, node in relation with item check in item_host_view
- Upload: DB lookup + nodes have right to upload

User

- Download:
  - Is owner of the item
  - Belongs to management egroup of this item
  - Is root on any machine assigned to the item



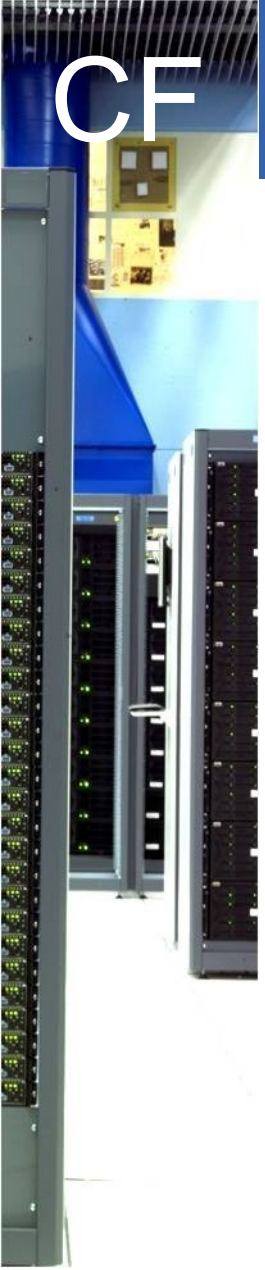
4. Authorization 2

User

- Upload:
  - Is owner of the item
  - Belongs to management egroup of this item
  - Nodes are allowed to upload
    and user has root on any machine

  - Any root is allowed to upload
    and user has root on any machine

  - Any LanDB user is allowed to upload
    and user is LanDB user on any machine



Thank you

We would be glad to receive any feedback from You!

jan.dudziec@cern.ch

CERN IT
Department
CH-1211 Geneva
23
Switzerland