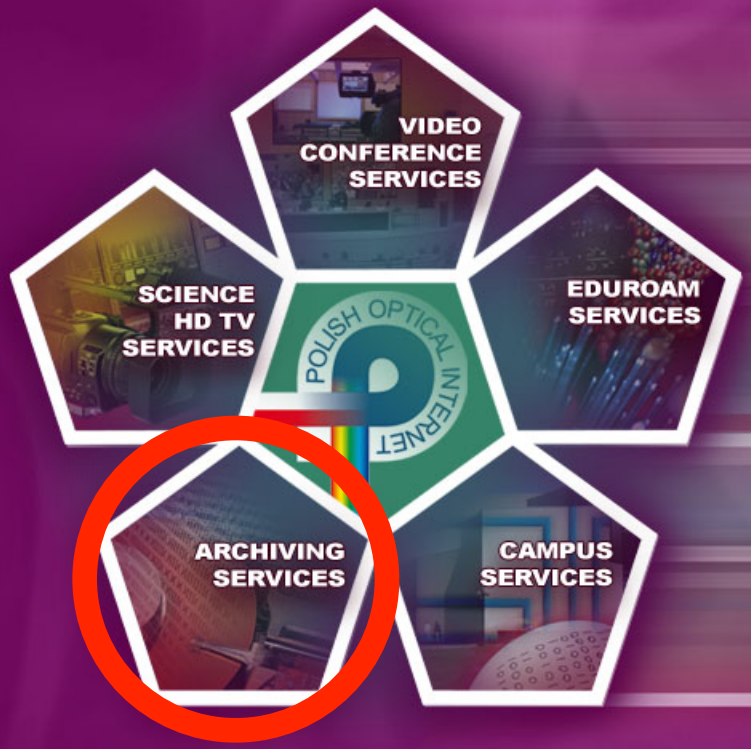
SERVICE PLATFORM FOR E-SCIENCE PLATON

www.platon.pionier.net.pl



Polish National Data Storage

Norbert Meyer, Maciej Brzeźniak, Maciej Stroiński

PSNC

INNOVATIVE ECONOMY
NATIONAL COHESION STRATEGY

POZNAN

European Union
European Regional Development Fund

Project nr. POIG.02.03.00-00-028/08

GRANTS FOR INNOVATION

Project co-financed by the European Union under the European Regional Development Fund

Workshop on Big Data and Open Data, Brussels. May 7-8, 2014

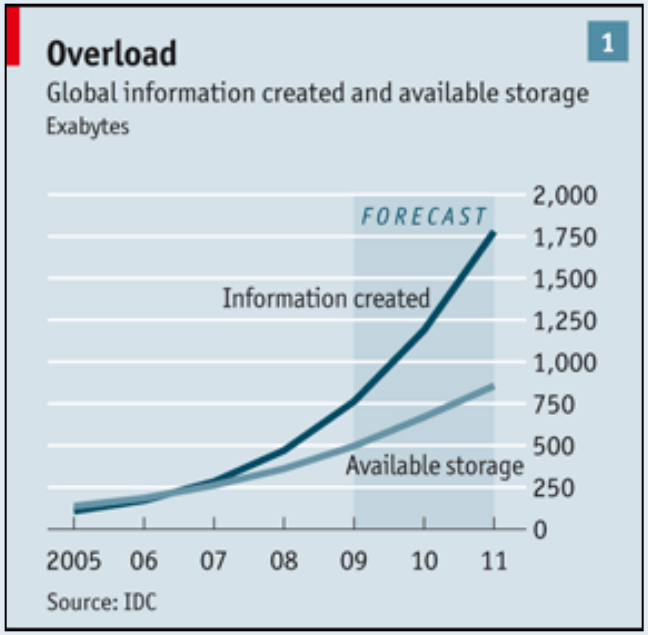
Data = value => needs protection

- **Data is value:**
  - Expensive research results
  - Priceless cultural heritage:
  - Data needed for organizations / projects to operate

=

- **Some of these data need protection!**

Data production worldwide (IDC):



In Poland:

Country:	PB's of data /year
Digital library:	100's of TB/year
Individuals:	100's of GB/year

Data archiving/backup is complex

- **Limited media durability:**

5-10 years

5-10 years

10 years?

15-30 years
(5000 mount)

- **Limited technology lifetime**

IBM 350 (1956)

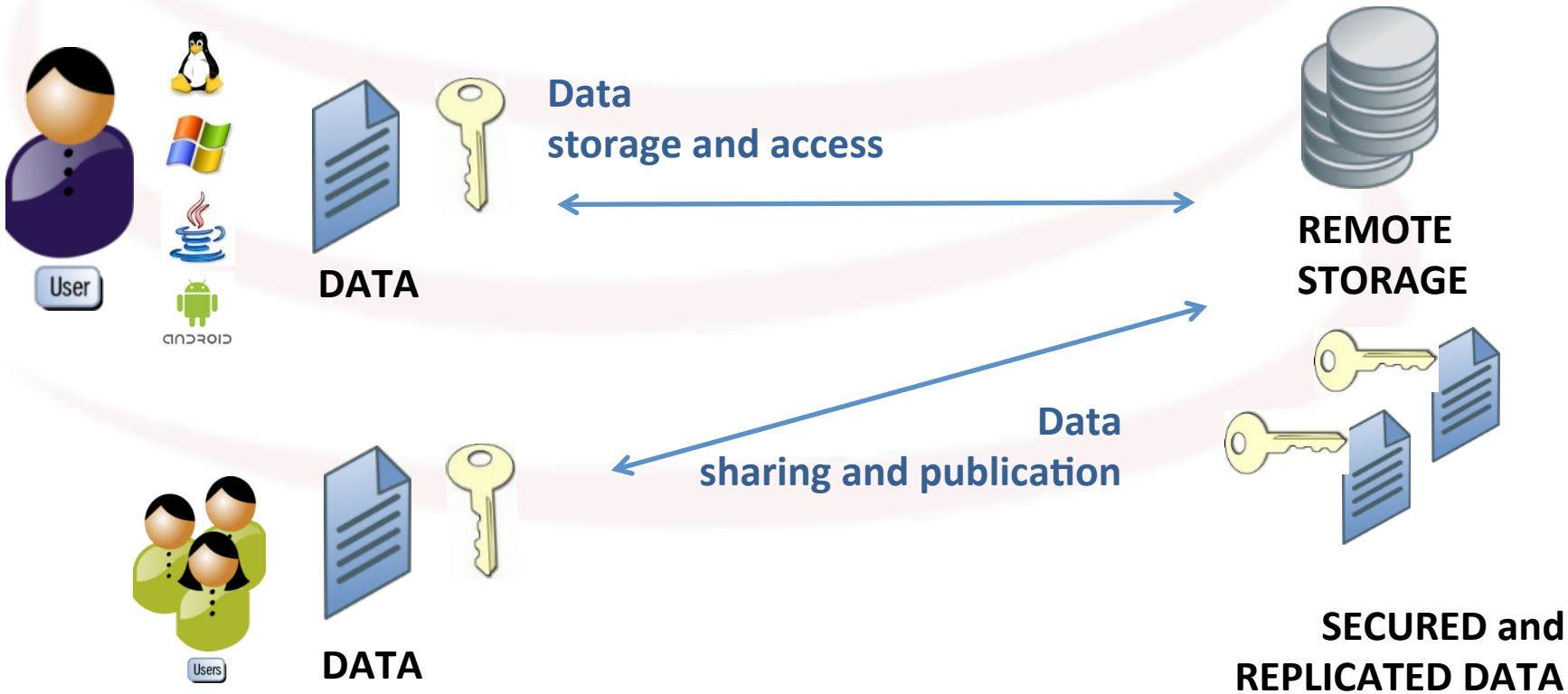
3,5" hard drive
(Rodime, 1986)

SSD (1995, M-Systems)

- **Costs, complexity, lack of know-how**

NDS2: use cases

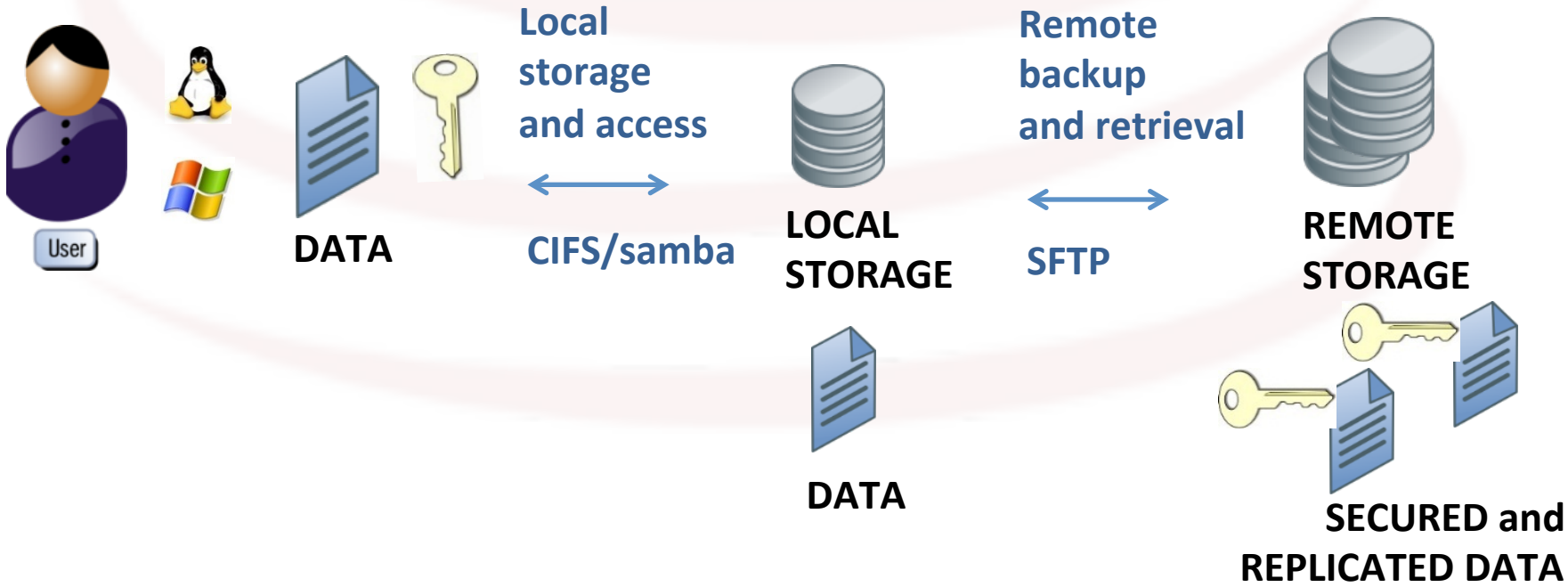
1. **Individual user** (scientist, researcher, student):
   - Data to be **available, persistent** and **safe**
   - **Easy and efficient access** to data from **various OSs**
   - I want **transparent** safety and security mechanisms
   - I want to **share** my data and be able to **publish** them



NDS2: use cases

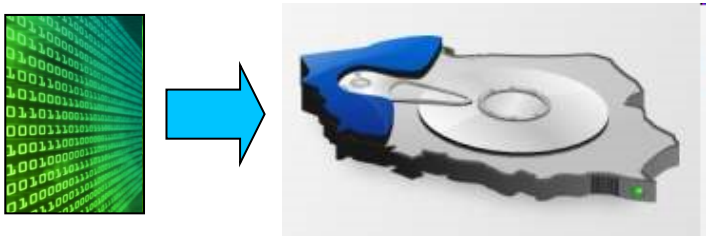
2. Institution, workgroup (digital library, scientific project)

- My data must be **available, persistent** and **safe**
- **I need a local working space** with **simple** and **efficient access** through **typical LAN protocols** (CIFS, NFS)
- Local space should be **extended by a remote space**



Solution: outsourcing to PLATON project

- **Added values:**
  - **Trusted service provider**
  - **Collaboration history**
  - **Knowledge & experience**
  - **Availability & proximity:**
    - Redundant infrastructure
    - Broadband network to universities
    - and research centres
  - **Additional services**
    - IdP, AAI



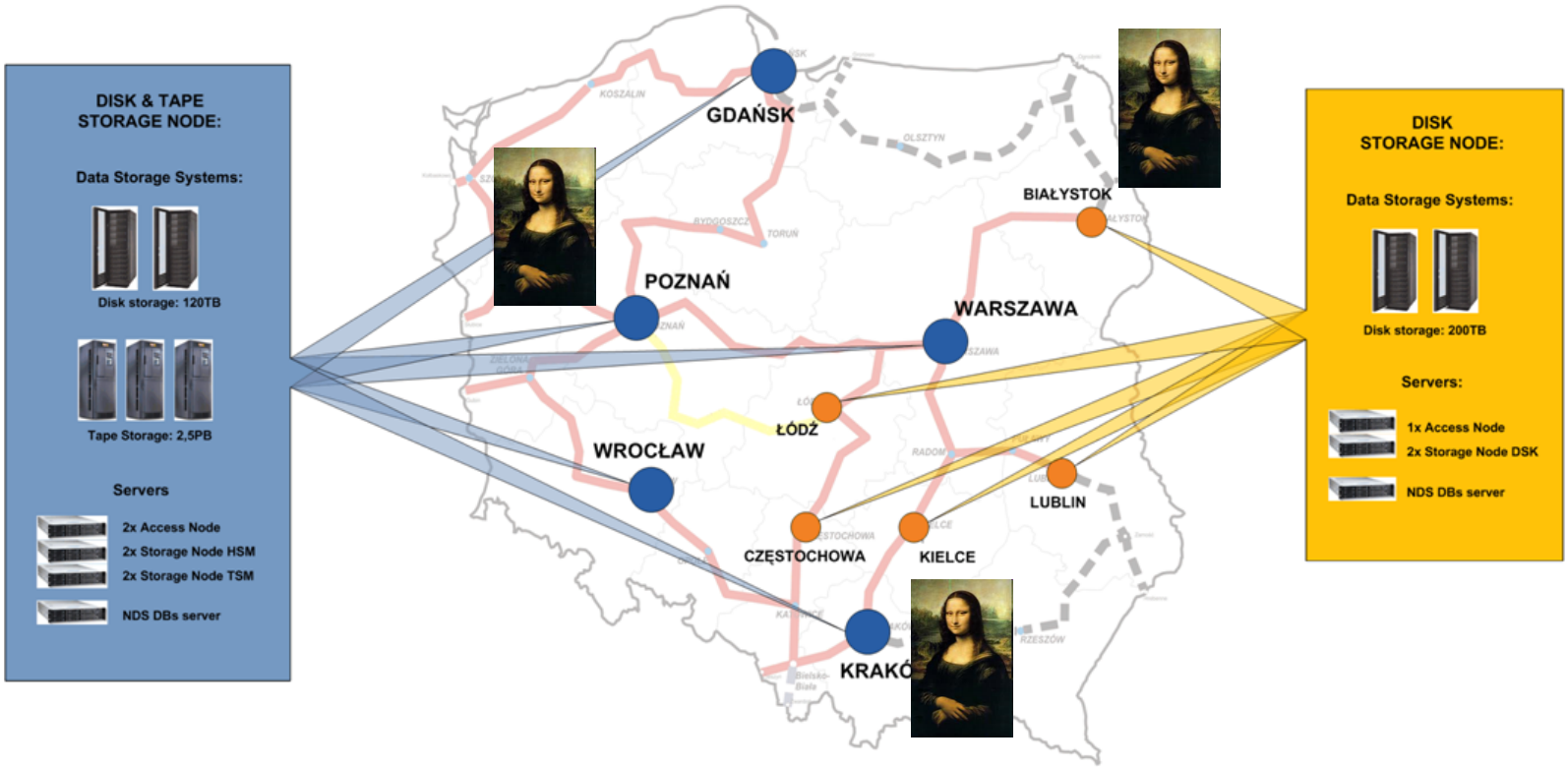
Data

PLATON-U4 service

The infrastructure

storage redundancy & high capacity

- **Multiple sites, geographically distant data centres**
- **Data replicated over the sites**
- **Storage resources: 12,5 PB** of tapes; 2 PB of disks



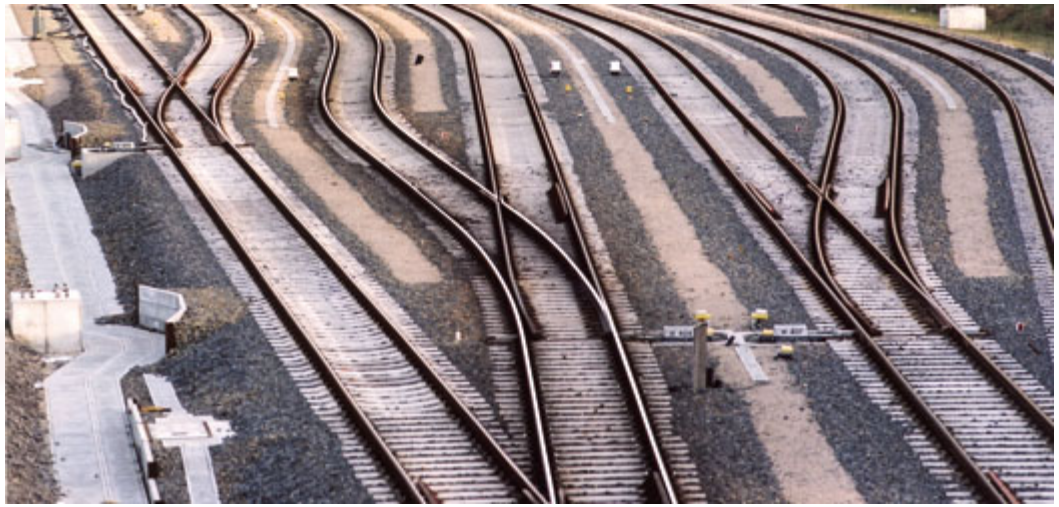
NDS2: problem definition

NDS2: secure, efficient and easy to use

NDS2 | National Data Storage

To provide at the same time:

- Data provided on a safety and secure way
- Efficiency of data storage and access
- Transparency of safety and security mechanisms
- Data sharing support
- Support for data publication



Requirements addressed by NDS platform

NDS2 National Data Storage

Features	Comments
Data availability & persistency	Replication, consistency checks
Basic security	Transfer encryption, access control at rest, policies (media degaussing)
Data sharing within a group	Server-side Linux filesystems mechanisms for access control
Easy and efficient access	Access to data through number of protocols: SFTP, WebDAV, Web GUI, GridFTP
Safety mechanism transparent & scalable	First replica created by user using a convenient protocol; then replicas created async. using GridFTP for efficiency in WAN

NDS2
a secure and extended NDS

- **NDS and PLATON experience:**
  - Replication, data persistency etc. – OK!
  - **Encryption and integrity control needed!**
    - Manual implementation too complicated
    - Existing tools not good enough
  - System shoud better integrate with user's system (Win, Linux, mobiles…) and institution / workgroup environment

- **NDS2 (2011-2013): National Data Store 2:**
  - **End-to-end encryption & integrity control**
  - **Easy and efficient data exchange**
  - Virtual disks for Windows, Linux
  - Appliance for institutions
  - Portable GUI client for individuals

NDS2

NDS2 National Data Storage

Features	Comments
End-to-end security: privacy & integrity	AES-256 for data, RSA for key exchange, SHA digests
Easy access, safery mechanisms transparency	Client-side cryptography provided by easy to use clients: virtual filesystems, Java GUI
Rollback and versioning	Server-side versioning + support in clients
Easy, efficient and secure data exchange	Symm. and assym. key hierarchy, key exchange mechanisms
Mobile access	Android application
Efficient & easy local storage & access + remote backup	Appliance for institutions

NDS2 cryptography:
encryption, integrity control and keys management

NDS2 cryptography: encryption, integrity control and keys mgmt (1)

NDS2 National Data Storage

Overall concept:

- Data encrypted with AES-256 CTR
  - AES - Strong and high performance algorithm for bulk data, resistant to brute force attacks
  - Hardware supported: Intel Westmere and ARMv8
  - Performance: 1-2,5 GB/s on todays workstations
  - CTR mode enables parallelism

- Integrity control by SHA-512:
  - Resistant to collisions and attacks
  - Calculated:
    - User-side (per 64kB logical block) in order to enable users to detect manipulations or corruption on data or their digest
    - System-side (per file) for replica integrity control

NDS2 cryptography: encryption, integrity control and keys mgmt (2)

NDS2 National Data Storage

- **Client-side encryption and integrity control:**
  - AES 256 CBC generated per file – for data privacy
    - Stored in the file header on the system side
    - **Protected with user's private RSA key**

    => User takes care of only 1 pair of keys
  - SHA-512 digests calculated per logical 64-byte block
    - Stored with each block on the system side
    - **Protected by encryption using files' symetric key**

    => User application may access digest information using file's AES key

file header	data chunk 1	data chunk 2	
516 Bytes	64 kBytes	64 kBytes	
Version (4 Bytes), { symmetric key+ NONCE, header digest } encrypted with RSA 4k	{ Data length in this chunk (4 Bytes) SHA512 block digest (64 Bytes) User data (65468 Bytes) } encrypted with AES and file symmetric	{ Data length in this chunk (4 Bytes) SHA512 block digest (64 Bytes) User data (65468 Bytes) } encrypted with AES and file symmetric	…

NDS2 cryptographic clients:

Features & concept:

Implementation,

Clients for NDS2 (1)

NDS2 National Data Storage

Windows users

CryptoFS 4Windows

- **FS-like access** (.net CallbackFS)
- **Encryption & digests** (.net crypto API)
- **SFTP client** (Rebex SFT library)

Linux users

CryptoFS 4Linux

- **SSHFS extension**
- **FS-like access** (FUSE/SSHFS)
- **Encryption & digests** (OpenSSL)
- **SFTP client** (Built-into SSHFS)

Work-groups

Appliance

- **LAN access through CIFS** (Samba server)
- **FS-like access** (CryptoFS 4 Linux)
- **Admin. interface** (php + perl)
- **Local disk storage**

WAN (SFTP)

NDS filesystem
(extended with versioning, ACLs)

SECURED and REPLICATED DATA

Clients for NDS2 (2)

NDS2 National Data Storage

Any platform

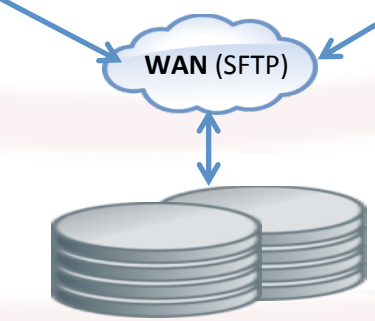
Java GUI, CLI and API

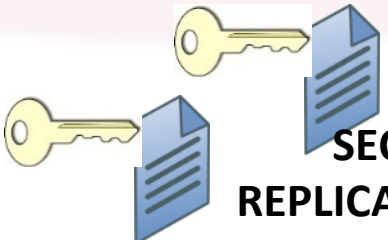
- Browser-like access
- Drag & dropp
- Encryption & digests (Bouncy Castle)
- SFTP client (JSCH sftp)
- Metadata search

Mobile platform

Android client

- Browser-like access
- Encryption & digests (Java API)
- SFTP client (Java API)
- Integration with Android shell





SECURED and REPLICATED DATA

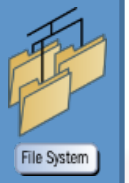
Clients for NDS2 (3)

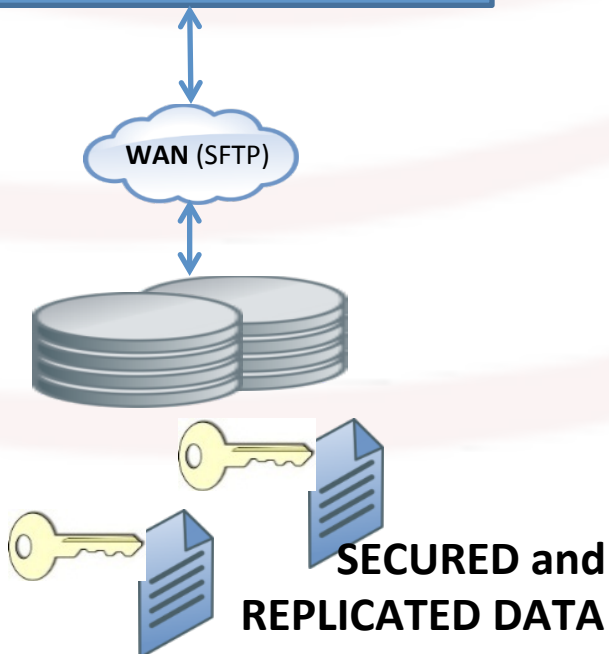
NDS2 National Data Storage

Dropbox-like functionality

Experimental data sync client 4 Windows:

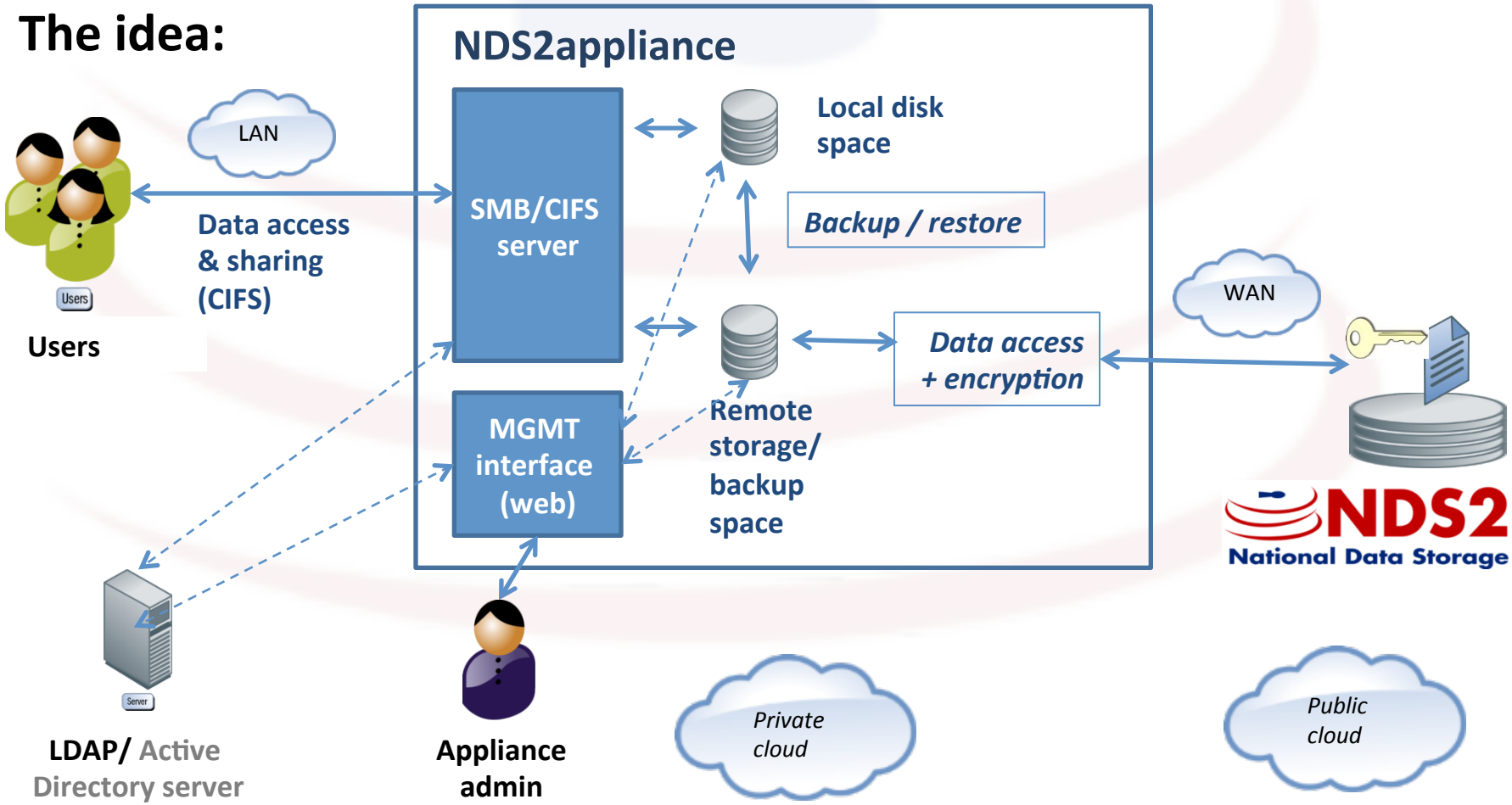
- Based on CryptoFS4Win components
- MS Synchronisation Framework for synchronisation





NDS2: appliance concept

- **Use cases:**
  - Small institution / workgroup shares data using local NAS appliance
  - Data protected against disaster and intrusion: backup and encryption
  - Remote space is a backup of local; local is cache of remote
- **The idea:**

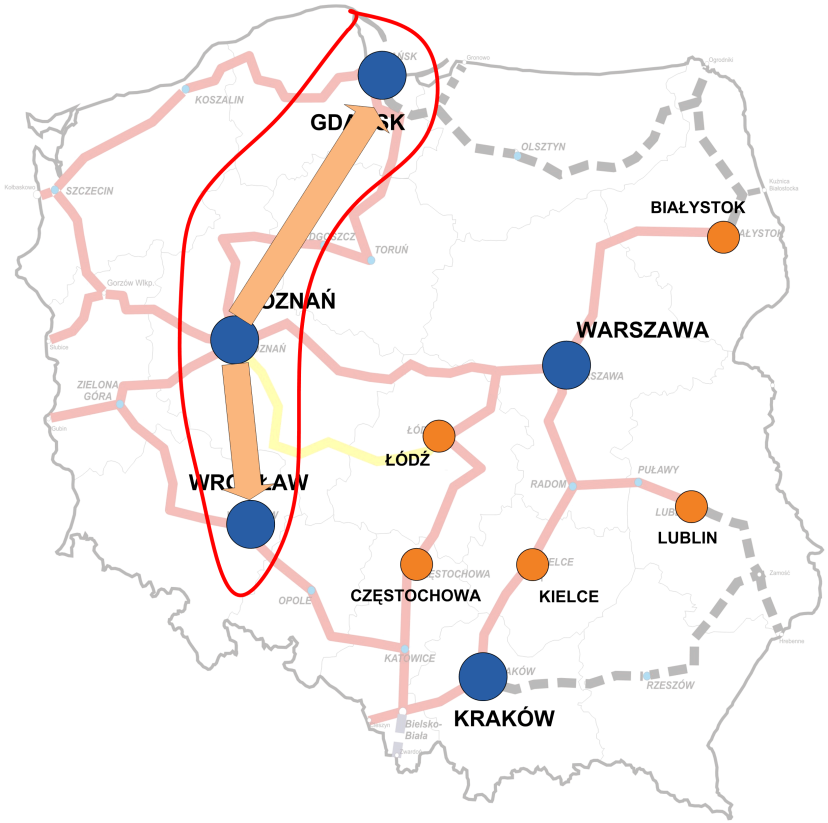


NDS in PLATON (3)

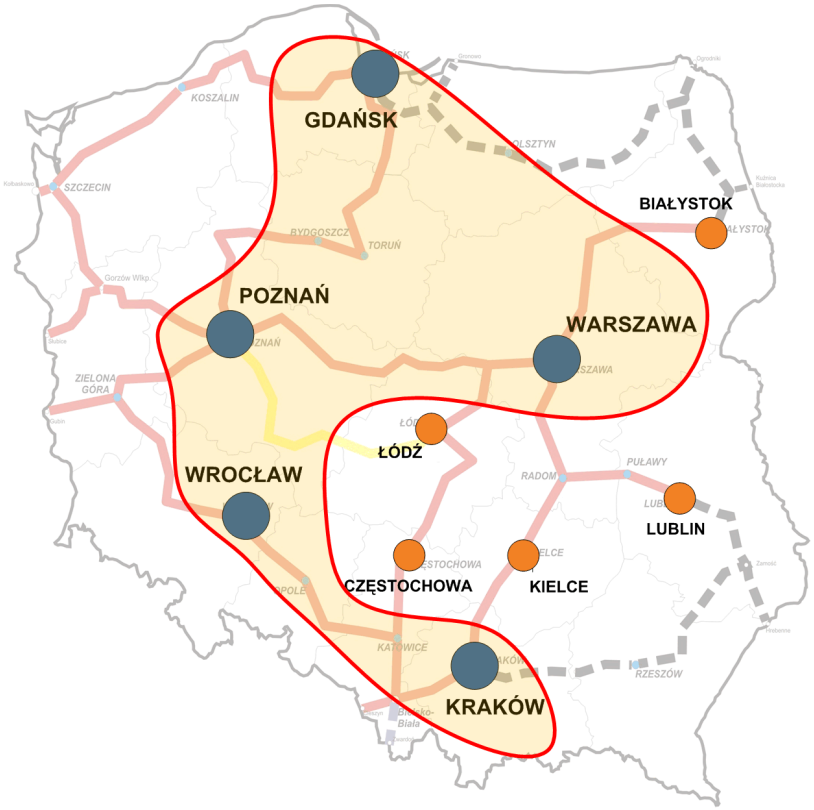
Sites vs system instances (1)

- **Example instances: PZ1 and WA1**

Regional instance

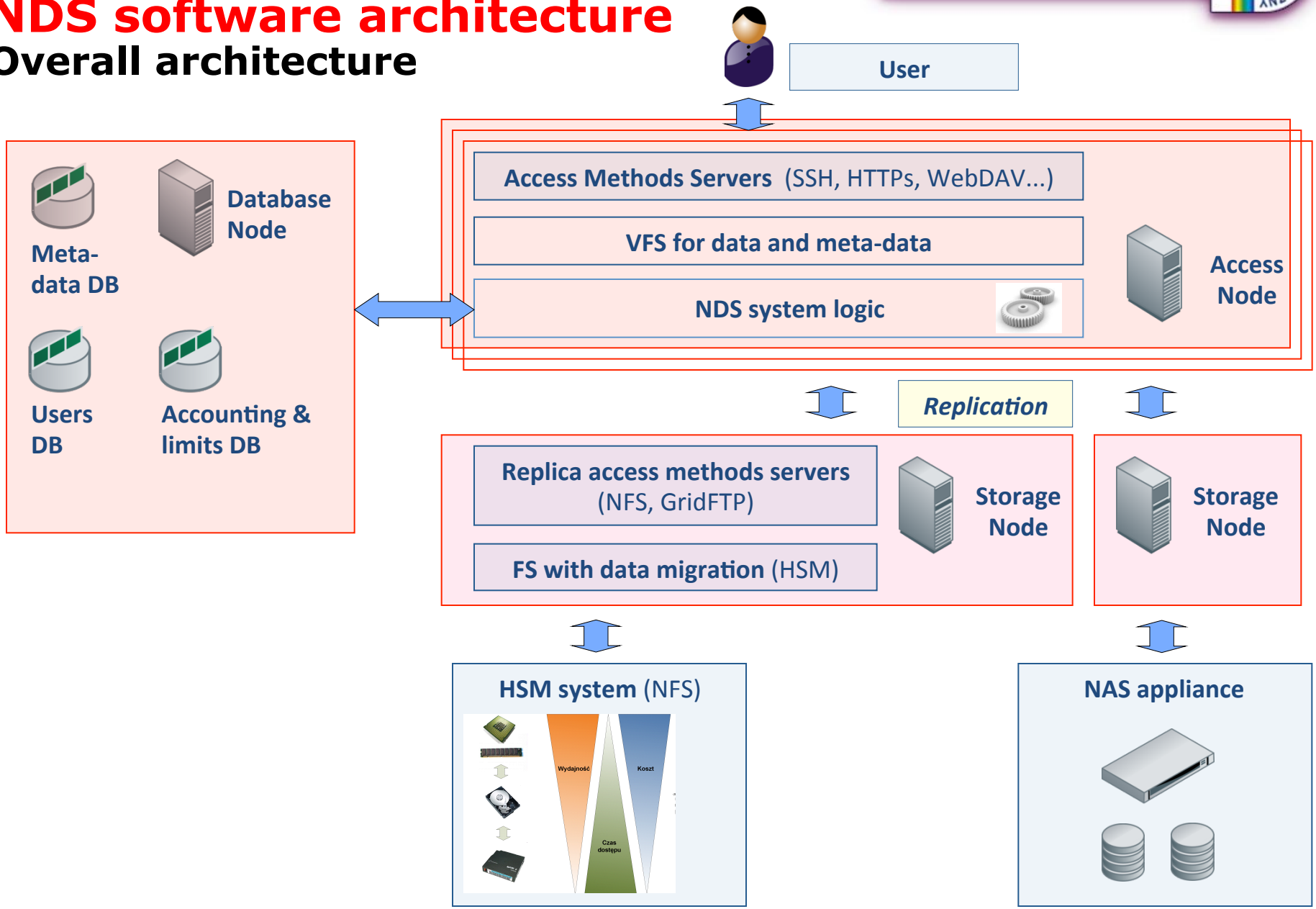


Project-dedicated instances



NDS software architecture

Overall architecture



PLATON's PAS infrastructure:
Tape & Disk Storage sites (15+ PB)

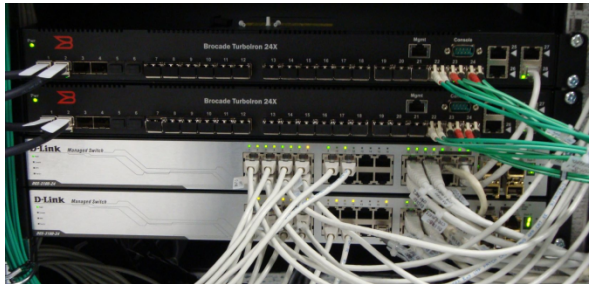
IBM TS3500 Tape library in Poznan

PLATON's PAS infrastructure:
Tape & Disk Storage sites

IBM DS5300 AND DS5100 disk arrays in Poznan

TSM/HSM storage servers

Access Node and Database Node servers



10 Gbit and 1 Gbit switches

Summary

NDS2 National Data Storage

- National service
  - as an added value to the network connection
  - or independent

- Base for the 'Common Data Services'
- Provided for individuals … SMEs … universities
- Worked out sustainability policy

SERVICE PLATFORM FOR E-SCIENCE PLATON

www.platon.pionier.net.pl

COORDINATOR:
INSTITUTE OF BIOORGANIC CHEMISTRY
POLISH ACADEMY OF SCIENCES
POZNAŃ SUPERCOMPUTING AND NETWORKING CENTER
ul. Noskowskiego 12/14, 61-704 Poznań,
Phone: (+48 61) 858 20 00,
fax: (+48 61) 852 59 54,
e-mail: **office@man.poznan.pl**,
www: **http://www.man.poznan.pl**

INNOVATIVE ECONOMY
NATIONAL COHESION STRATEGY

European Union
European Regional Development Fund

Project nr. POIG.02.03.00-00-028/08

GRANTS FOR INNOVATION

Project co-financed by the European Union under the European Regional Development Fund