10. Fachkongress des IT-Planungsrates am 9. und 10. März 2022 im Saarland

Verwaltung für das 21. Jahrhundert –
einfach, agil, digital, krisenresillient

Herzlich willkommen!

max planck institut informatik

MAX PLANCK INSTITUTE
FOR SOFTWARE SYSTEMS

Technische Aspekte der Digitalisierung

Verlässliche IT als Basis für

exzellente Wissenschaft und

digitalisierte Verwaltung in der MPG

Jörg Herrmann

Max Planck Institute for Informatics
Max Planck Institute for Softwaresystems
Saarland Informatics Campus
Joint Administration
IST (Information Services and Technology)
Head IST - Max Planck Institute for Informatics
Head IST-Core

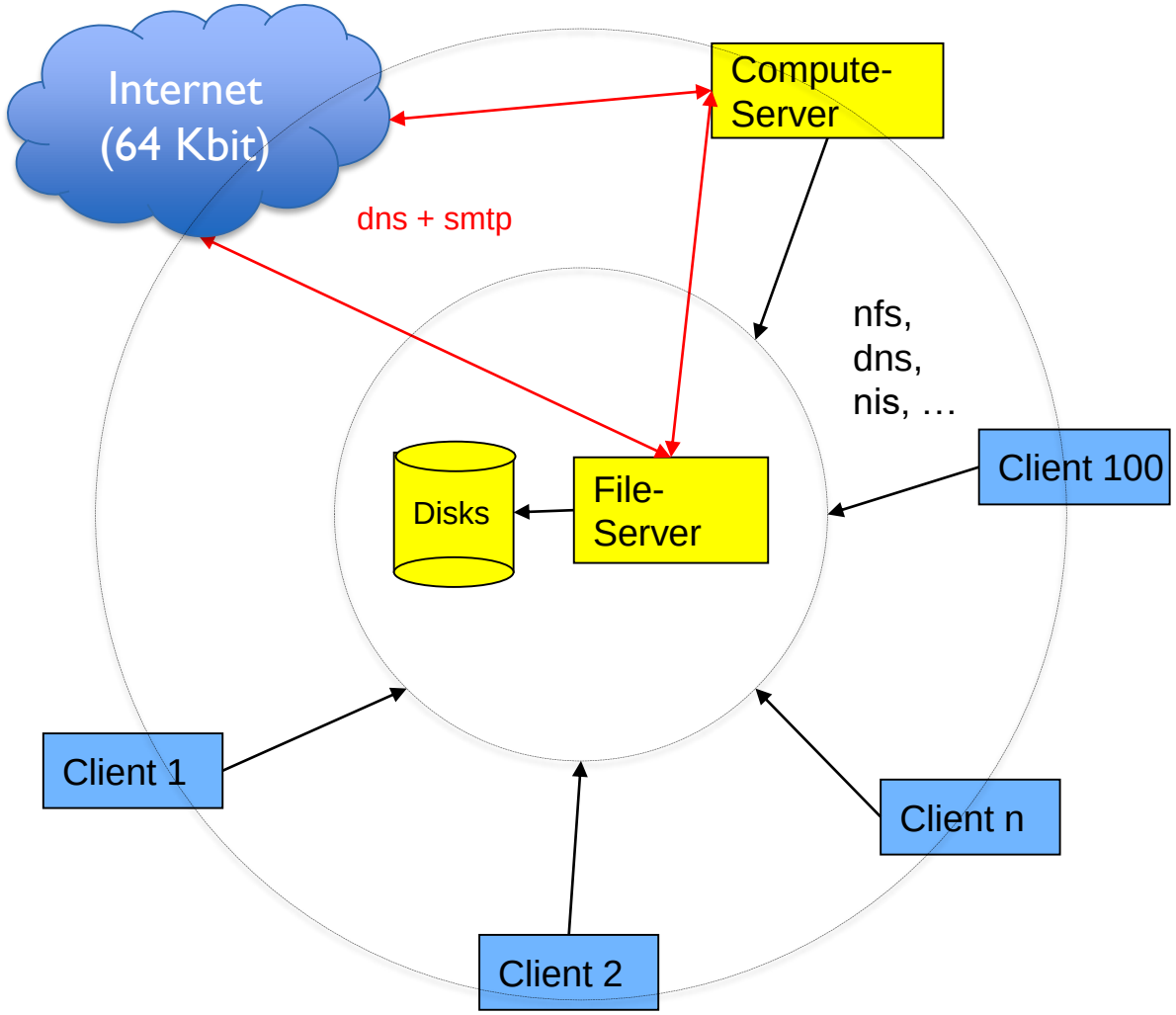
Die Max-Planck-Institute am Standort

- Die Max-Planck-Gesellschaft hat derzeit 86 Institute
- Zwei MPIs am Standort mit gemeins. Verwaltung, Technik & IT
  - MPI für Informatik (seit 1990 in Saarbrücken)
    - widmet sich Algorithmen und ihren Anwendungen im weitesten Sinne – die Forschung reicht von den Grundlagen (Algorithmen und Komplexität, Programmierlogik) bis hin zu einer Vielzahl von Anwendungsbereichen (Computergrafik, geometrische Berechnungen, Lösen von Beschränkungen, Programmverifikation, Datenbanken und Informationssysteme sowie Computerbiologie/Bioinformatik).
  - MPI for Software Systems (seit 2004 in Saarbrücken und Kaiserslautern)
    - untersucht die Prinzipien effizienter, zuverlässiger, sicherer und benutzbarer Computersysteme sowie deren Interaktion mit dem physischen und sozialen Kontext, in dem sie arbeiten. Wir betreiben Grundlagenforschung in relevanten Bereichen der Informatik und darüber hinaus, die Theorie, empirische Analysen und datengestützte Untersuchungen umfasst.

Ausgangssituation

- Bereits 1990 war “alles” abhängig von der IT-Infrastruktur
  - Typisch: 1 – 2 große Maschinen als Server:
    - Am Ende fast alles abhängig von einer Maschine, keine technischen Alternativen
  - Zeitlicher Kontext:
    - Microsoft brauchte Novell etc. für IDM und Fileservice
    - Unix-Derivate noch nicht ausgereift – Dauerbetrieb unmöglich
    - Linus Thorwalds spielte noch mit Lego-Bausteinen
  - **setzte Maßstäbe für Verlässlichkeitsanforderungen**
    - Mangelhafte Zuverlässigkeit und Performance von Disks, Netzwerk, Betriebssystemen etc. führte zur Unzufriedenheit
    - Besser ab etwa 2006 mit Cluster-Konzepten, ZFS von SUN, Fibre-Channel, schnellerem Ethernet und immer mehr Linux als Client- und Server-Betriebssystem

Typisches Setup für kleine Institute



- Sehr **einfaches** Setup
- **aber nicht verlässlich**
  - Stillstand bei
    - Ausfall einer Disk, eines Bandlaufwerks
    - einem Kernel-Problem
    - einem Netzwerk-Problem
- **weder ausreichend skalierbar noch optimierbar**

Verlässlichkeit und Digitalisierung

Verlässlichkeit in guten wie in schlechten Zeiten!

- Verbesserung der staatlichen Krisenresilienz durch Digitalisierung
- Erhöhung der Handlungsfähigkeit durch Reduzierung von Komplexität
- Erfahrungen aus der Corona-Pandemie: Mut zu mehr beherztem Aufgreifen von Chancen
- Agilität als Schlüssel für eine erfolgreiche Verwaltung
- KI und Cybersicherheit als wesentliche Technologien

Verlässlichkeit im Kontext von

- Verbesserung der staatlichen Krisenresilienz durch Digitalisierung
- Erhöhung der Handlungsfähigkeit durch Reduzierung von Komplexität
- Erfahrungen aus der Corona-Pandemie: Mut zu mehr beherztem Aufgreifen von Chancen
- Agilität als Schlüssel für eine erfolgreiche Verwaltung
- KI und Cybersicherheit als wesentliche Technologien

Verlässlichkeit ⊂ Resilienz

- Wiederholbarkeit
- Passgenauigkeit
- Homogenität
- Flexibilität, Agilität, Skalierbarkeit
- Verfügbarkeit
  - Robustheit
  - Widerstandsfähigkeit
- Sicherheit
  - Unabhängigkeit

Was bedeutet das für die IT?

Passgenauigkeit

- User resp. Projekte wählen den passenden “Einstieg” in den Dienstleistungsstack (Ebene)
  - Alle Ebenen bis dahin sind Service der IT
  - Alle höheren Ebenen liegen in der Verantwortlichkeit der User. Die IT macht dort Best-Effort ohne Garantien
- Minimale Ebene ist Hardware
  - die IT ist immer für Netzwerk und Asset-Lifecycle zuständig
    - technische Auswahl … Inventarisierung … Anschluss … Wartung … Aus

	Dienstleistungsstack
7	Programmierte Applikation (eher für Projekte)
6	Konfigurierte Applikation (z.B. virtual host)
5	Applikationen (z.B. Web-Server)
4	Filesysteme, Datenbanken, Backup + Archive
3	Betriebsystem mit oder ohne Accounts
2	Hardware
1	Netzwerk

Wiederholbarkeit

- Digitalisierung (Automatisierung) der IT als Basis für Wiederholbarkeit
  - kategorien-basierte Konfigurations-Datenbank als Basis jeder Maschinen-Installation (vom Notebook bis zum Server-Cluster)
    - Umfasst DNS, DHCP, LDAP, Betriebssystem- und Softwareinstallation sowie elementare Konfigurationen
  - Nutzung von Softwareverteilung (cfengine → ansible) und Versionierungssystemen (CVS, SVN, GIT) als Basis von Konfigurationsänderungen
    - Nutzung der entsprechenden Automatismen (cfengine, ansible, Debian Paket-System) bei der Installation und bei der täglichen Konfiguration garantiert Funktion
    - Vergleichbares bei den Autoinstallationen und Autokonfigurationen von Windows- und macOS-Systemen
    - Backup von Standard-Systemen nahezu überflüssig, weil sie identisch reproduziert werden können (Backup für lokale Log-Files, Command-History und in Ausnahmen lokale Daten der Administratoren)
  - manuelle Installationen sind Test-Installationen zur Vorbereitung von Services
- Beschränkt auf die Infrastruktur resp. den von der IT garantierten Bereich
  - Ausnahme: die Projekte verwenden die Mechanismen der IT (selten)
    - Backup von Notebooks und Projekt-Servern hat hohen Stellenwert, auch Backup und Archiv wiss. Daten

Homogenität

- beim Einsatz von Programmen, Applikationen, etc.
  - beim Übergang von Notebooks auf leistungsfähigere Umgebungen
  - identische Betriebssysteme und – versionen
  - identische Applikationen von Notebook, Workstation bis hin zum Server-Cluster
- für die Nutzung wissenschaftlicher Daten
  - bei der Nutzung unterschiedlichster Plattformen
  - Daten von der Workstation bis zum Server-Cluster mit identischem Pfad
    - Unter Linux am Notebook und bei Windows und macOS über SMBFS etc. verfügbar
- für die Arbeit an Dokumenten
  - bei der Nutzung von Maschinen mit verschiedenen Betriebssystemen
  - durch Alternativen (z.B. OpenOffice) als lokale Apps oder in Kollaborations-Plattformen

Flexibilität, Agilität, Skalierbarkeit

- Die Digitalisierung der IT reduziert den Gesamt-Aufwand
  - Sie ist Garant für spontane, schnelle und leichtfüßige Installationen
  - Sie ermöglicht schnell realisierbare Test-Szenarien wegen des geringeren Arbeitaufwandes
  - Selbst der Aufwand für unwesentliche Änderungen lohnt sich in der Summe
  - Digitalisierung bzw. Automatisierung fördert die **Flexibilität**
- Die Digitalisierung der IT macht Änderungen sofort für alles nutzbar
  - Sie unterstützt mit jeder “schnellen” Fehlerkorrektur die Verbesserung des Gesamt-Systems
  - Sie verstärkt mit jedem Erfolg die Verlässlichkeit des und das Vertrauen in das Gesamt-System
  - Digitalisierung bzw. Automatisierung ist die Basis von **Agilität**
- **Skalierbarkeit** durch Erhöhung der Anzahl **an “optimaler” Stelle**
  - z.B. File-Server-Cluster, Server, Disks, Verbindungen zu den Netzwerken
  - z.B. Anzahl der Compute-Cluster, Server, Speicher, …

Verfügbarkeit

- 99,9 % inkl. geplanter Wartungen als Zielsetzung für einzelne Services
  - **kein hartes Ziel** aber Basis für Systemdesign ohne Wartungsfenster
- Hohe Verfügbarkeit nur erreichbar mit Redundanzen
  - im WAN
    - Redundante Internet-Anbindung und Verbindung der Standorte,
  - im LAN (Ethernet) und SAN (Fibre Channel)
    - Doppelte Verkabelung, auch zur Steigerung des Durchsatzes
  - in der Stromversorgung und im Klima
    - N+1 als Versorgungskonzept (Raid 5) für USV und Klima
    - Server und Netzwerkkomponenten mit doppelten Stromversorgungen
    - Schränke mit USV-Strom und Haushaltsstrom versorgt für getrennte Versorgung der Netzteile
- … und großer Robustheit der Services

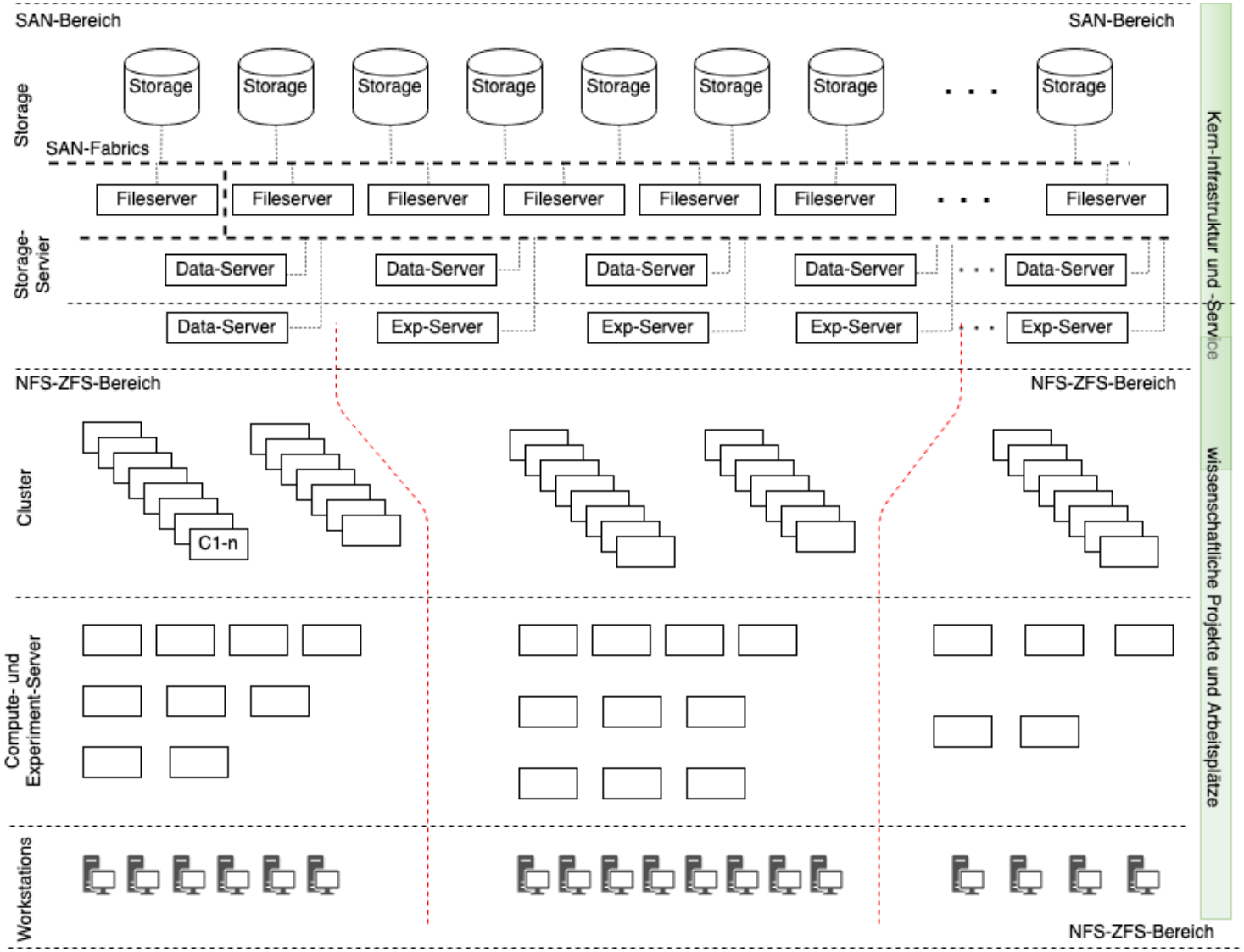
Robustheit (Beispiele)

- Wartung freigestellter Systeme
  - Kritische Systeme (File-Service, Mail-Service, ...) bestehen aus unabhängig wartbaren Teilsystemen
    - z.B. im File-Service teilen sich mehrere Server ein Set von SAN-Devices. Zu wartende Systeme werden von Filesystemen befreit. Sukzessive Wartung aller Server ohne Downtime für die Clients.
- Betrieb von Funktionseinheiten
  - Dienste, die stark von anderen Diensten abhängen, werden mit diesen Diensten zusammen betrieben
    - z.B. DNS-Server werden aus dem Konfigurations-System betankt und begleiten jeden stark auf DNS basierten Dienst (wie z.B. E-Mail)
- Keine aufgesetzte High-Availablity bei Daten-Services
  - Krisensituationen können durch Missverständnisse der HA-Komponenten entstehen und Daten zerstören
- Kein absolutes Vertrauen in Raid-Arrays
  - Serverseitige Spiegelung von Raid 6 ermöglicht konsequente Ausnutzung doppelter Verkabelung und kaschiert sogar vollständigen Ausfall eines Raid-Arrays
  - Das Filiesystem (hier: ZFS) übernimmt Check-Summing von File-Systemen und die Garantie für korrekte Daten

Widerstandfähigkeit (Beispiele)

- Reduktion der Komplexität durch modularen Aufbau
  - z.B. nicht ein File-Server für alles sondern in Bezug auf Betriebssicherheit, Durchsatz und Größe skalierbares System
    - Ca. 20 Cluster aus vorwiegend 4 Servern und entsprechendem Storage
    - Eigene Management-Tools zum last- oder wartungsbedingten Umzug der File-Systeme im Cluster
    - Spezielle File-Systeme für hohen Durchsatz in Server-Clustern (BeeGFS)
- Verlagerung riskanter Schnittstellen an beherrschbare Stellen
  - z.B. erfülle die Anforderungen von Clients
    - AD zur Versorgung von Microsoft-Komponenten, LDAP zur Versorgung von Linux-Systemen
    - IDM-System betankt AD und LDAP
- User-Anforderungen gezielt unterstützen
  - z.B. drei Betriebssysteme
  - z.B. zwei Mail-Front-End-Systeme
    - Groupware-Aspekte können im imap-Umfeld nicht zufriedenstellend gelöst werden
    - Wissenschaftler wollen universelle Schnittstellen, Groupware-Systeme sind zu speziell

Skalierbare Infrastruktur



Sicherheit (Ein “Aber” für Selbstverständliches)

- Backup (ist selbstverständlich ;-)
  - Banana (Backup-Analyse)
    - macht Test auf Vollständigkeit – Wertet verfügbare Filesysteme und Backup-Logs aus
  - Aktives Notebook-Backup
    - sucht regelmäßig “seine” Notebooks und beginnt Backup sofort; Server warnt per E-Mail den Nutzer bei ausbleibendem Backup
  - Online Mail-Stream-Backup
    - Jeder, am E-Mail-Service beteiligte Server, speichert jede durchlaufende E-Mail zwischen
    - Konzipiert gegen fehlerhafte Konfigurationen; genutzt gegen übervolle private E-Mail-Postfächer
- System-Logs (sind verteilt und groß)
  - Zentrale System-Uhr und zentrales Syslog für zeitliche Koinzidenz
  - Log-surfer erkennt Annomalien und meldet sie
- Firewalls (trennen Gut und Böse)
  - Was ist gut und was ist böse? ➔ Services müssen sich selbst beschützen ➔ Strikte Trennung
    - User haben nur das Recht, Services zu nutzen, nicht aber den Server
    - Server bieten nur einzelne geschützte Dienste an (getrennte File-Server, Mail-Server, Web-Server, Compute-Server, ...)

Sicherheit (optimierte Nutzung)

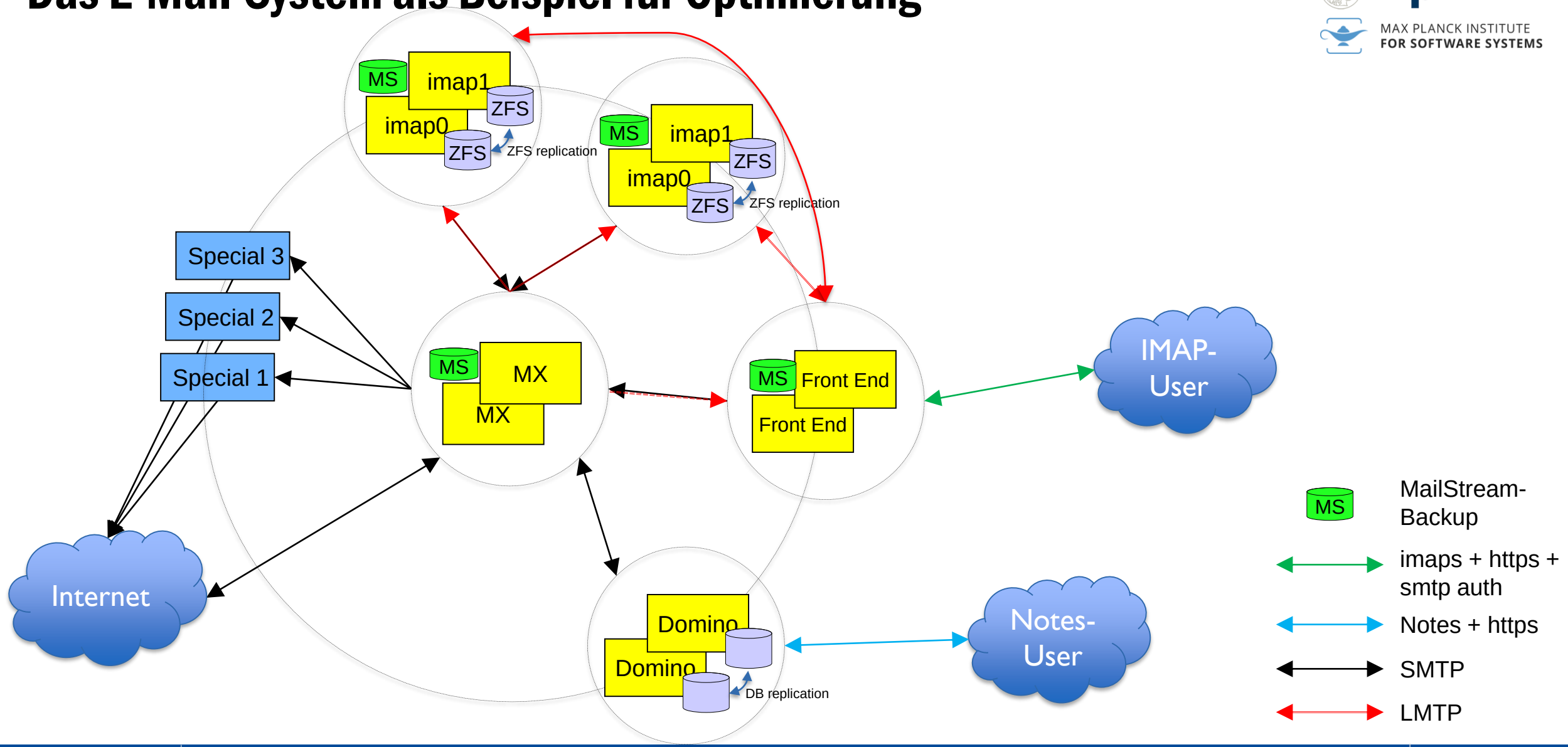
- Alternative Hardware-Anbieter – optimiert nach Kompatibilität
  - Multi-Vendor-Strategie bei Hardware und Software (wo möglich)
- Alternative Betriebssysteme – Einsatz optimiert nach Anforderungen
  - Linux auf Notebooks, Workstations, Servern und Serverfarmen (Cluster)
  - Windows auf Notebooks, Workstations und Servern
  - MacOS auf Notebooks und Desktops
- Alternative Applikationen – Einsatz optimiert nach Anforderungen
  - MS-Office, Collabora (OpenOffice), Only-Office, LaTeX
  - Adobe Acrobat und alternative PDF-Apps
  - ShareLaTeX in sandstorm & Overleaf, nextcloud & Confluence, Codimd, ethercalc, etherpad, moinmoin, codimd
  - Jitsi, BigBlueButton, Cisco und Zoom

Sicherheit (Optimierung und Souveränität)

- Alternative Mail-Systeme
  - Nicht ein komplexer (intransparenter, kommerzieller) E-Mail-Service* sondern spezialisierte, einzeln optimierbare E-Mail-Teil-Services
- Vermeidung von Monopolisten als Lieferanten (Souveränität)
  - Nicht ein Service vom Monopolisten sondern ein imap-basierter Service mit einer kommerziellen Alternative mit ausgeprägten Groupware-Eigenschaften
  - Nicht nur AD, sondern ein IDM-System mit Anschluss an AD, LDAP, ...
  - Kein überkomplexes kommerzielles IDM-System als zentrale Infrastrukturapplikation sondern eine eigenentwickelte skalierbare Lösung auf Basis von Opensource-Tools
  - Keine intransparente komplexe kommerzielle NAS-Lösung sondern eine modulare, skalierbare und transparente OpenSource-FileService-Lösung

* der zukünftig nur in der Cloud sicher betrieben werden kann

Das E-Mail-System als Beispiel für Optimierung



Résumé

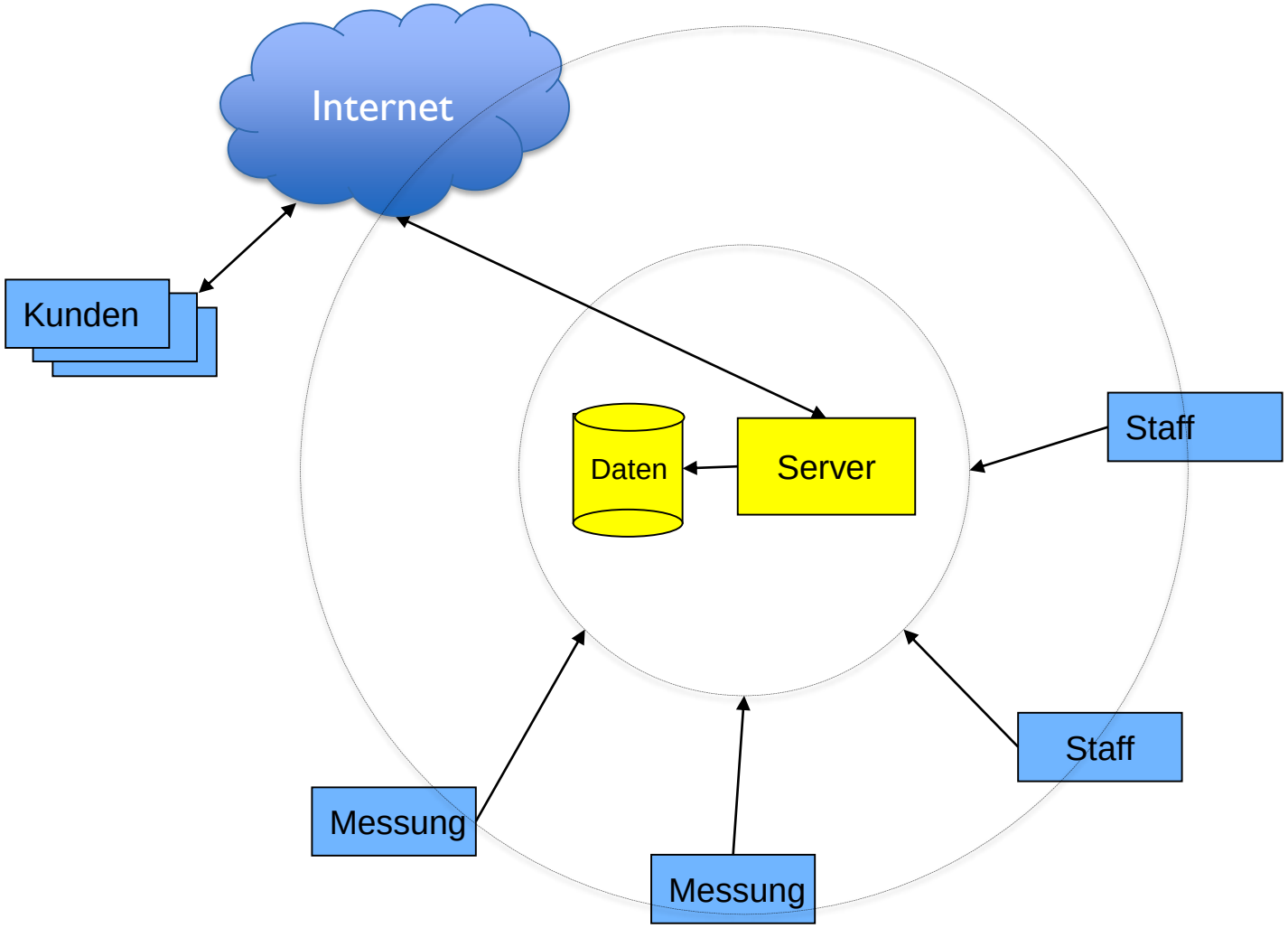
- Das resultierende System ist verlässlich
  - Seit Jahren keine wirklichen Ausfälle
  - wartungsbedingte Ausfälle können verhindert werden
  - nur Ausfälle beim Verursacher (gutes “failure containment”)
  - Alternativen erleichtern Optimierung der Arbeitsprozesse
- Das Gesamtsystem ist modular, flexibel und skalierbar
  - Einzelne Komponenten sind einfach
  - Skaliert wird meistens durch die Anzahl der Komponenten
- Das Gesamtsystem ist komplex alleine wegen seiner Größe
  - Mehr “Digitalisierung” widerspricht in gewissem Sinn der “Reduzierung der Komplexität”
  - Aber: Divide & Conquer – die einzelnen Module sind gut beherrschbar

Was bedeutet das für die Digitalisierung?

Implikationen für die Digitalisierung

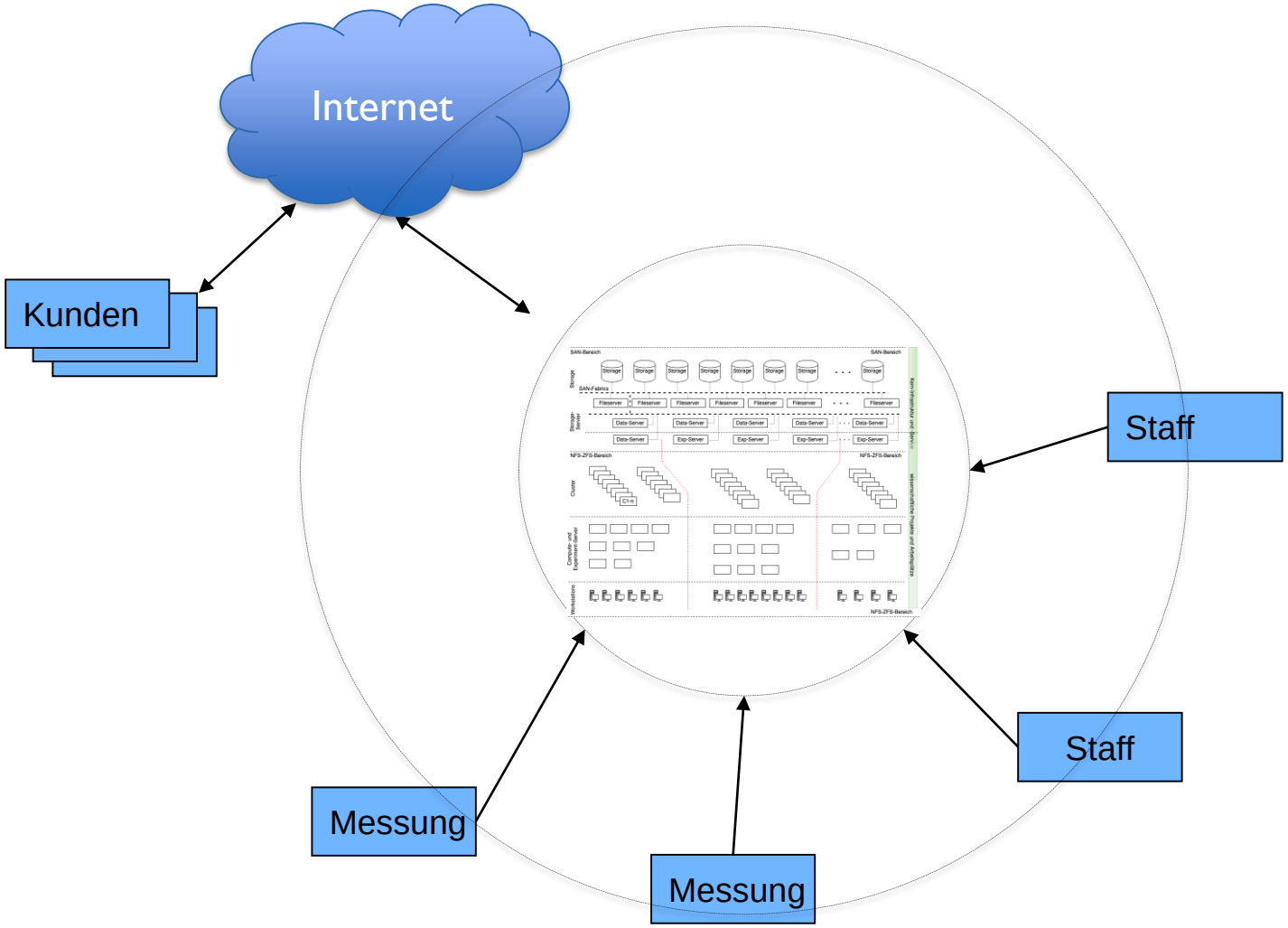
- Ihre Digitalisierung wird sich weiterentwickeln (und wachsen) – wie unsere Infrastruktur
  - “Migrationen” (im Sinne maßgeblicher Veränderungen) werden noch während der ersten Digitalisierungswelle anstehen
  - Ihre Infrastruktur wird sich dementsprechend weiterentwickeln können müssen
  - Das kann unter Umständen sehr schnell gehen (Corona-Anforderungen)
- Ihre Daten, deren Korrektheit, Verteilung und Aktualität werden ihr wichtigstes Gut sein
  - Sie werden Daten aus den unterschiedlichsten Quellen sammeln, zusammenführen und bearbeiten müssen.
  - Optimierte Eingabe- und Bearbeitungsverfahren werden der Schlüssel zum Erfolg sein.
  - Das betrifft Kund:Innen, Bearbeiter:Innen und technische Schnittstellen (z.B. Erfassung digitaler Ausweise)
- Sie werden auf die Daten externer Bereiche angewiesen sein und umgekehrt
  - Externe Kommunikationsprobleme sollten ihre Digitalisierung nicht blockieren (z.B. Ahrtal)
  - Ihre Infrastruktur muss in der Lage sein, das adäquat aufzufangen
- Ihre Digitalisierung wird zum (empfindlichen) Rückgrat der Organisation
  - Das gilt auch für die Infrastruktur für die Digitalisierung
  - Ihre Infrastruktur, deren Versorgung und ihre Kommunikationswege werden kritisches Betriebsmittel

Keine gute Idee



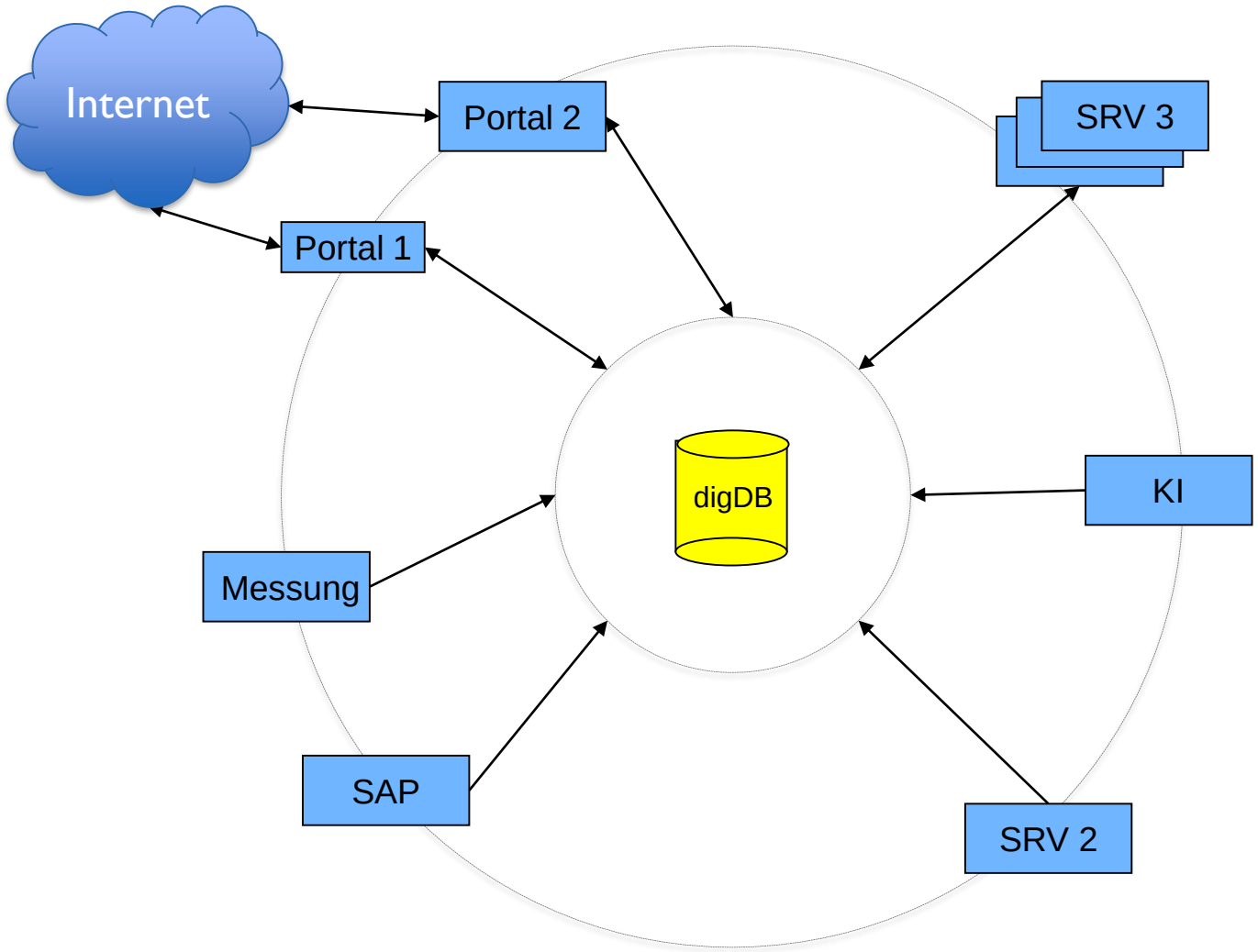
- Zu einfaches Setup
  - nicht “verlässlich”
  - weder skalierbar noch optimierbar

Besserer Ansatz



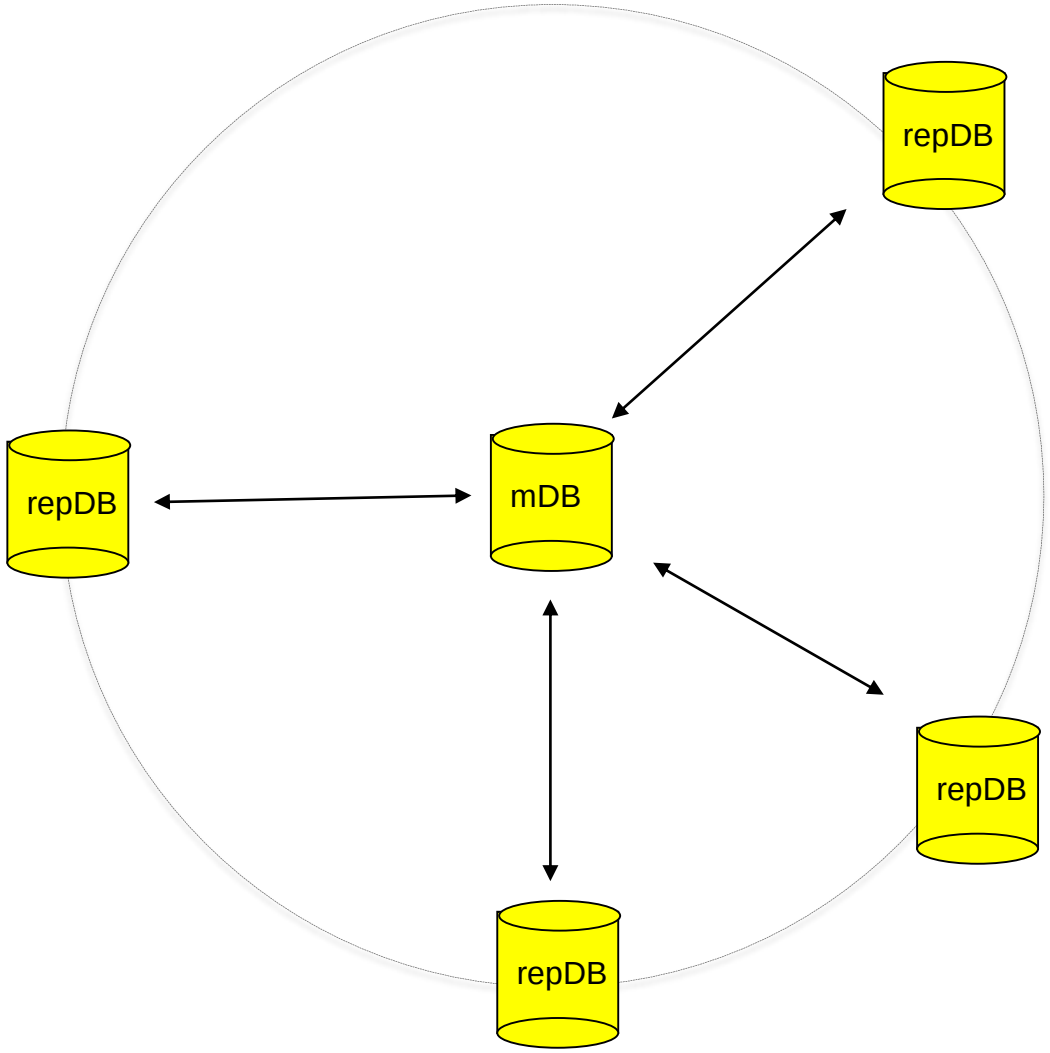
- Setzen Sie auf einen modularen Ansatz, der
  - “verlässlich”,
  - skalierbar und optimierbar ist.

Als eine Idee für einen Standort



- Verteilung von Daten triggert applikationsspezifischen Import
  - verlässlicher
  - skalierbarer und
  - optimierbarer

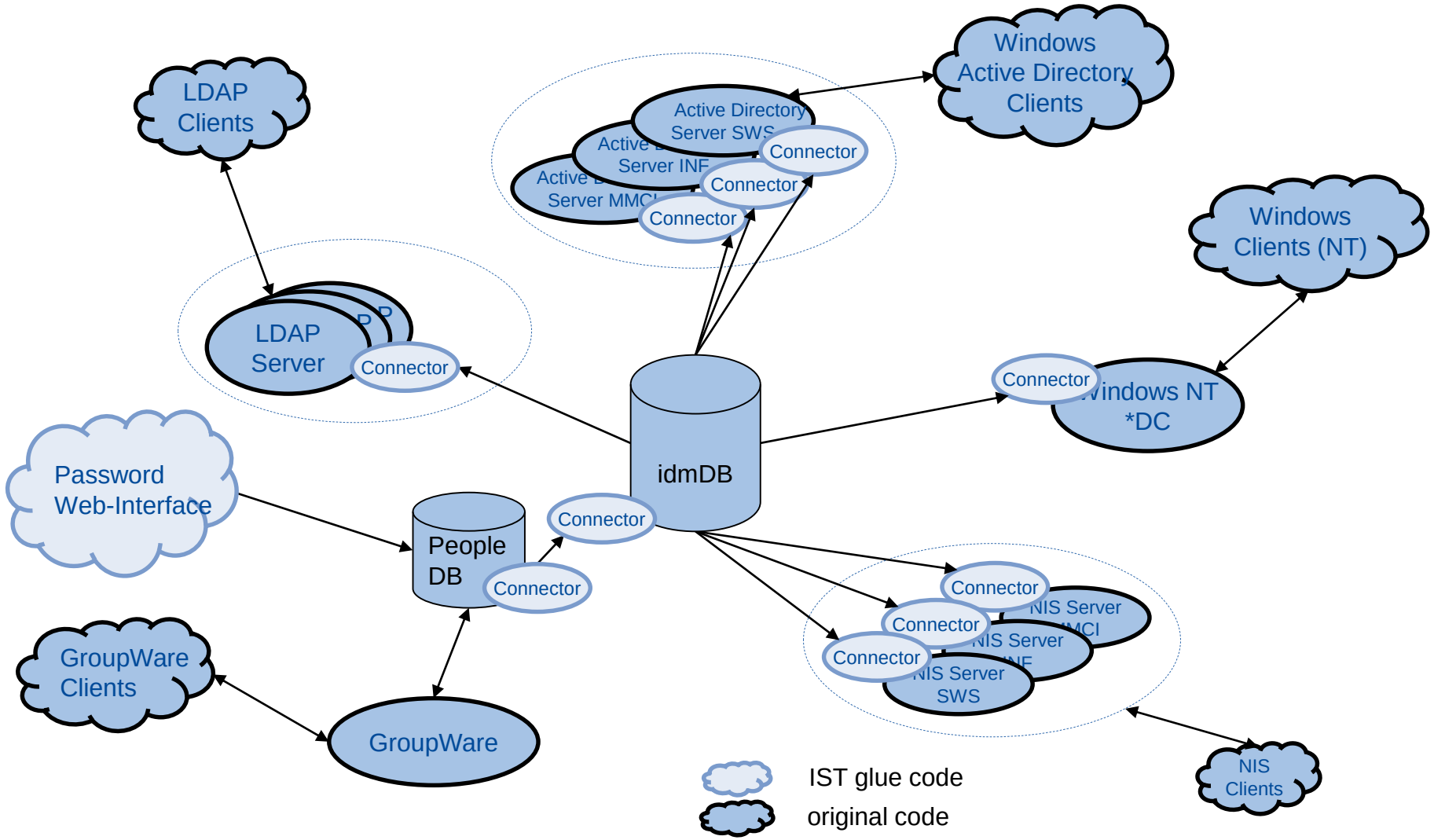
Als eine Idee für verteilte Standorte



- Upload von Daten in Master-DB (mDB) triggert Verteilung in Replikationen (repDB):
  - Bessere lokale oder regionale Verfügbarkeit
  - Fragen:
    - Asynchronität, Zugriffsrechte, führendes System, ...

Vielen Dank für Ihre Aufmerksamkeit.

Unser Identity Manager als Beispiel



Das System

- IT für
  - 900 Accounts, 464 mit Büroraum, 433 mit Telefonnummer
  - 2 Institute und Kooperationen in 5 Gebäuden in SB und KL
- Maschinen
  - 500 Workstations, Y Notebooks,
    - 75 Drucker, 538 Telefone ~ 20 Räume mit Videokonferenzanlagen
  - > 900 Server, > 500 virtuelle Maschinen, davon
    - 22 Windows-Server, 42 ESX-Server und
    - 73 Fileserver in 22 Clustern mit 2,25 PB Daten in 154 Pools in 1578 Filesystemen (max 22 TB Größe)
- Daten
  - insgesamt 10,6 PB auf 2888 Disks in 50 “Silos”
  - verteilt über Fileserver, über SAN und direkt angeschlossen
- Admins
  - Hardware + Betriebssysteme + Storage + Infrastrukturdienste (4 SA (Senior Adminstrator) +1 T (Techniker))
  - Interne & externe Netze + Telefonie + VC (2 SA + 1 T)
  - Applikationen (3 SA)
  - Service an 2 Standorten für 5 Gebäude (3 SA + 2 A (Administrator) + 2 T)

IT und Digitalisierung in ähnlichem Kontext

Deutschland	MPG
Bundesverwaltung	Generalverwaltung (GV)
16 Länderverwaltungen	86 Institute (Stand 1.1.2021)
Detaillierte Verteilung von Aufgaben zwischen Bund, Ländern und Kommunen	Detaillierte Verteilung von Aufgaben zwischen GV und Institutsverwaltungen
Länder und Kommunen unterschiedlich groß und unterschiedlich organisiert	Forschung ist Institutsaufgabe, lokale Verwaltungen unterstützen die Forschung, basierend auf den Regularien der GV
Vermutung: Die (verteilte) IT unterstützt staatliche und kommunale Anlagen, betreibt Infrastruktur und Services und ist damit die Basis für die Digitalisierung der Verwaltung	IT unterstützt maßgeblich Forschungsprojekte und betreibt Infrastruktur und Services und ist damit Basis für Forschung und Digitalisierung
Vermutung: teilweise erhebliche Unterschiede bei Anforderungen und beim Stand der Digitalisierung	Unterschiedliche Anforderungen implizieren unterschiedliche Digitalisierungsansätze und -stände – zentrale Ansätze müssen lokale Anforderungen berücksichtigen