EMI Support for EEF Requirements

Alberto Di Meglio (CERN)

Project Director

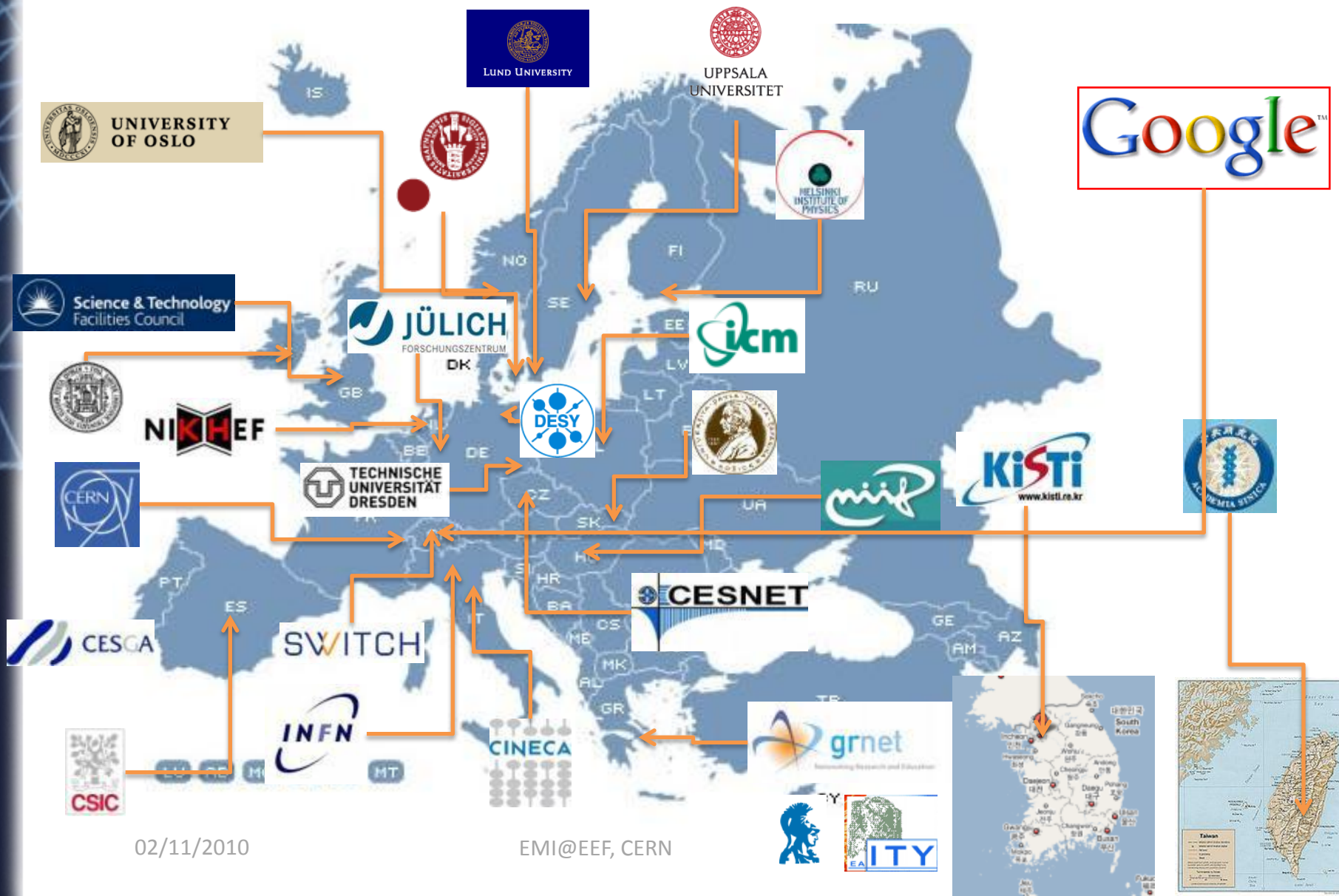
Outline

- EMI in a Nutshell
- The EMI Release Management Process
- EMI and EEF Requirements

EMI in a Nutshell

- Three-year project (May 2010-April 2013)
- Collaboration among ARC, gLite, UNICORE and dCache
- 2319 PMs effort provided by 26 partners, lead by CERN
  - 45% development
  - 35% maintenance and support
  - 20% administration, dissemination, training
- 24M € in total, 12M from the EC

Partners (26)


Lund University
Uppsala Universitet
University of Oslo
Google
Science & Technology Facilities Council
Jülich Forschungszentrum
icm
NIKHEF
DESY
CERN
Technische Universität Dresden
KiSTi
www.kisti.re.kr
CESNET
CESGA
SWITCH
INFN
CINECA
grnet
CSIC
ITY
IS
NO
SE
FI
RU
EE
LV
LT
DK
GB
IE
BE
DE
PL
UA
SK
HU
PT
ES
IT
SI
HR
BA
RS
ME
MK
AL
GR
GE
AM
AZ

Primary Objectives

Consolidate

Consolidate the existing middleware distribution simplifying services and components to make them more sustainable (including use of off-the-shelf and commercial components whenever possible)

Evolve

Evolve the middleware services/functionality following the requirement of infrastructure and communities, mainly focusing on operational, standardization and interoperability aspects

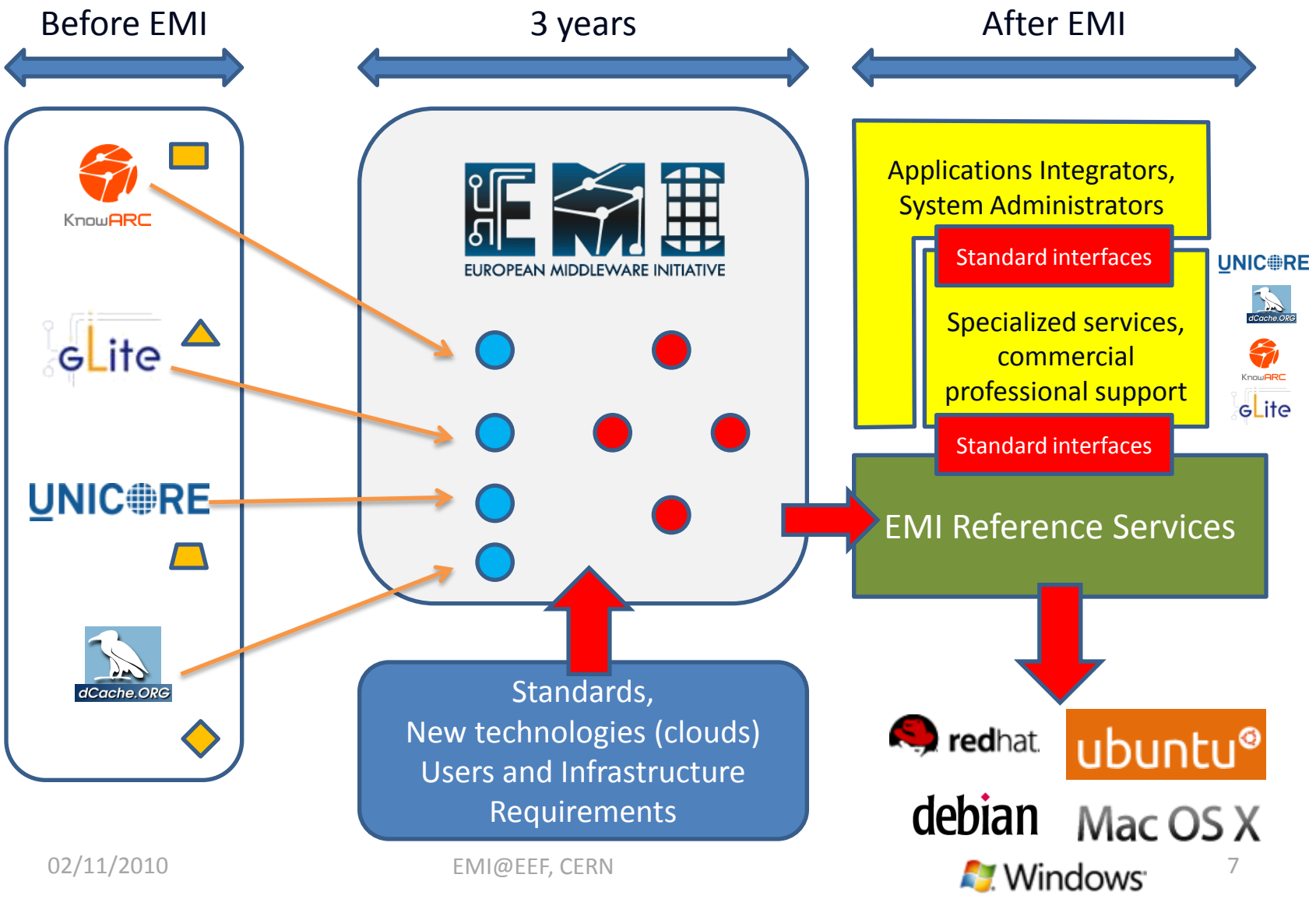
Support

Reactively and proactively maintain the middleware distribution to keep it in line with the growing infrastructure usage

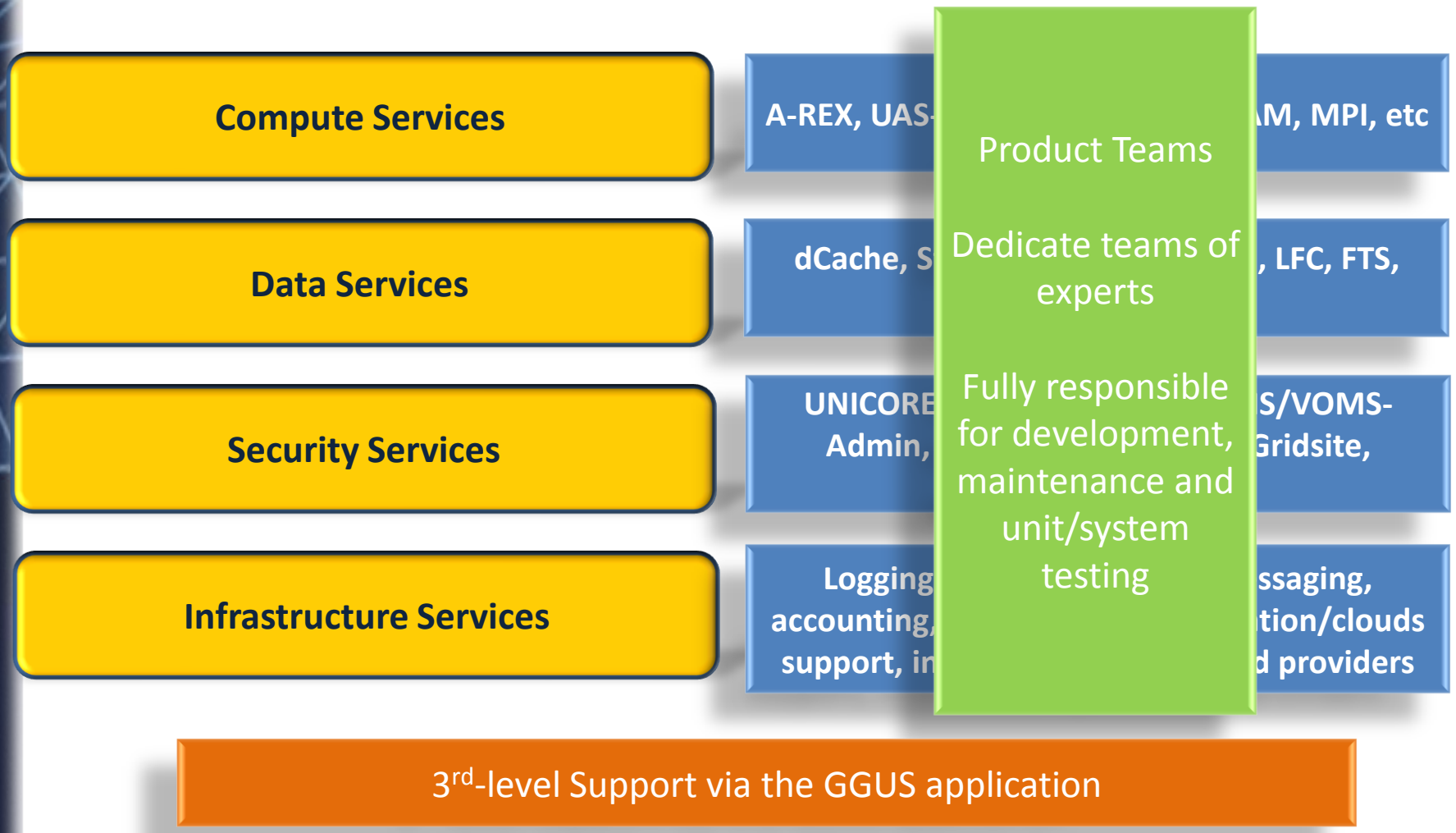
Outline

- EMI in a Nutshell
- The EMI Release Management Process
- EMI and EEF Requirements

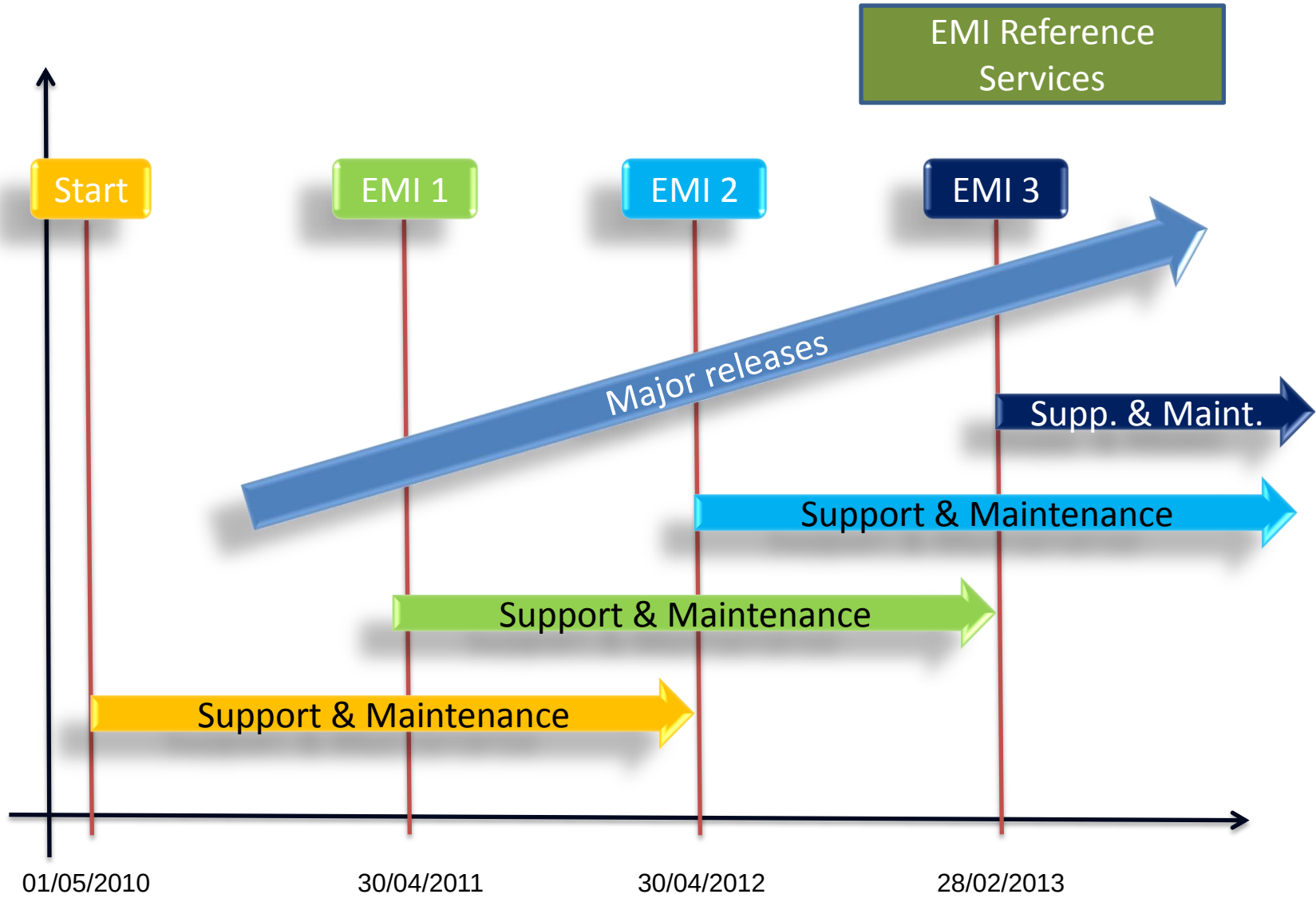
EMI Middleware Evolution



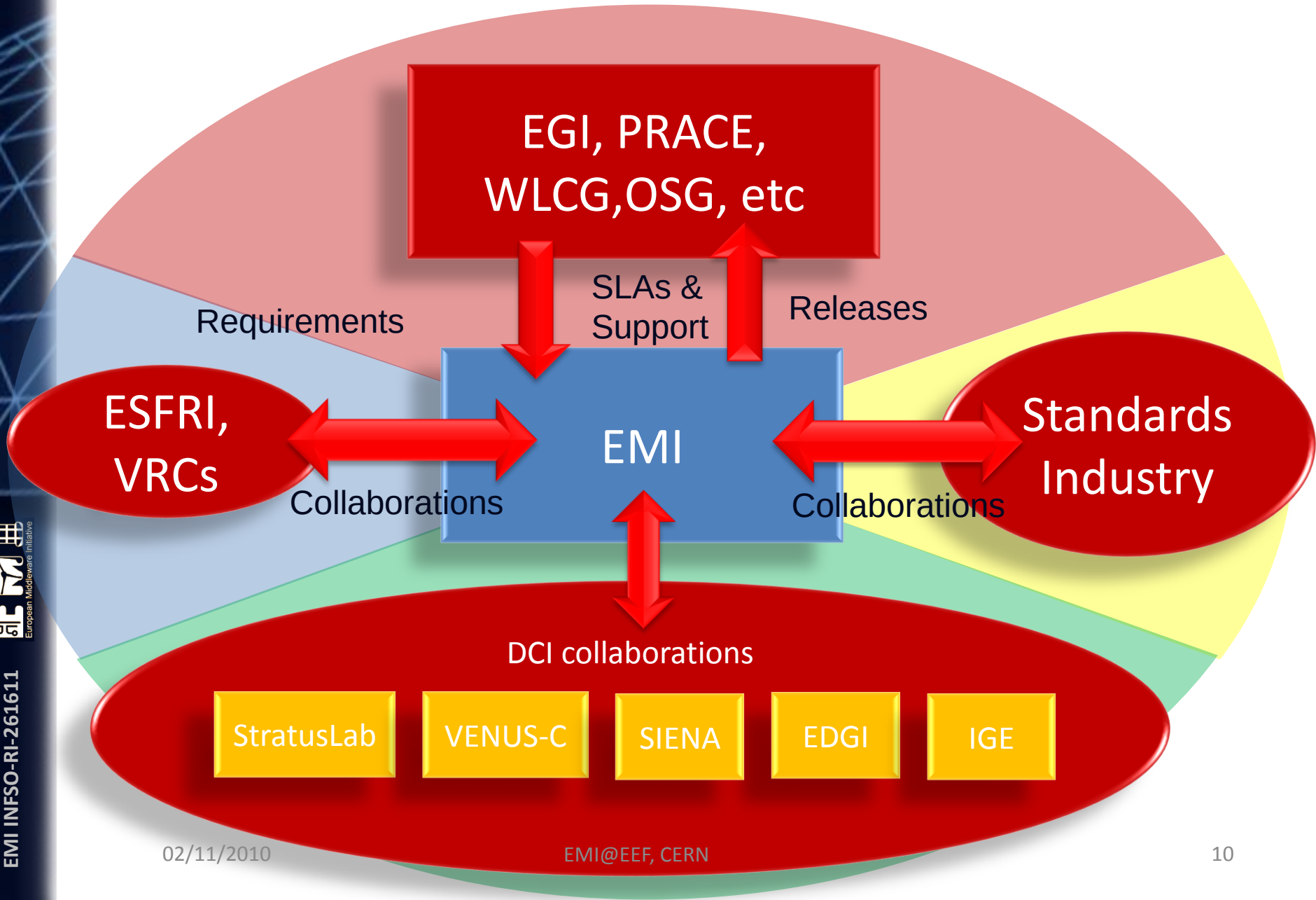
Technical Areas



Release Plan



Collaborations



Outline

- EMI in a Nutshell
- The EMI Release Management Process
- EMI and EEF Requirements

Single Sign-On (AAI)

- Refer to John White's talk for the technical details
- EMI addresses this requirement by:
  - Consolidating the security models across all EMI services and providing a common set of Authentication libraries
  - Supporting a common X.509 and SAML based Attribute Authority Service integrated with all EMI components
  - Reducing the complexities of handling certificates and integrating different security mechanisms like Shibboleth and Kerberos across the EMI stack
  - Refocusing the MSWG to concretely address security topics

Virtual Organizations

- EMI addresses this requirement by:
  - Supporting a common X.509 and SAML based Attribute Authority Service integrated with all EMI components (SAML-enabled VOMS)
  - Adopting a common agreed set of attributes to be used in authorization policies
  - Adopting a common Authorization decision mechanism and policies management services across the EMI stack (Argus)

Persistent Storage and IDs

- This requirement is not directly addressed by EMI, several other projects are or will work on this
- EMI is ready to address this requirement by:
  - Consolidating the File Catalogue functionality in a common service across all the supported EMI data management services (LFC)
  - Providing a common data client library (EMI_datalib) ready to support PIDs as soon as a model is established

Web Services

- All EMI services already provide a WS interface
- However there are important aspects that EMI is addressing:
  - Development of a single service registry across all EMI stack where all services can be registered no matter which specific distribution they belong to
  - Addition of service management ports to all EMI service to ease the service lifecycle management
  - Coherent adoption of standards whenever relevant (SRM, common Execution Service interfaces, a messaging framework, removal of httpg in favour of https, etc)

Workflows

- EMI does not develop any workflow application or tool
- However EMI supports the development of such tools by:
  - Providing consolidated programming interfaces across all services
  - Consolidating important areas like AA models, data and compute clients
  - Adopting agreed standards

Integration with Cloud

- Although EMI does not directly develop any cloud service, integration with emerging cloud technology is strategic
- EMI addresses this requirement by:
  - Integrating support for existing cloud systems like OpenNebula in its job management chain
    - Transparent use of dynamic resource allocation
  - Working with specific cloud projects like StratusLab and VENUS-C to understand
    - how grid services can be deployed with dynamic virtual environment
    - How existing grid functionality like authorization or accounting can be used by cloud services

Roadmap: timeline

- First phase, EMI-I
  - important technical agreements
  - consolidation plans for compute and data
  - design and early prototypes
  - additional new capabilities for production ready components.
  - EMI-1 release due April 2011.
- Second phase, EMI-2
  - consolidation plans for the remaining two areas
  - Some design and prototypes
  - Most intensive development phase resulting production ready features
  - EMI-2 due April 2012
- Third phase, EMI-Final
  - completing the consolidation plans
  - bringing the prototypes to production level
  - EMI-3 (or Final) release due April 2013

EMI phase 1 (2011 April)

- Agreements:
  - Execution Service interface
  - Accounting records (compute, storage)
  - Common security attributes
  - Common SAML profiles
  - Messaging use cases
  - Replacement of legacy GSI
  - EMI delegation
  - AAI ”strategy”
- Consolidation plans
  - Compute area clients & APIs
  - Data access libraries (EMI_datalib)
  - Common authentication library (EMI_authlib)
- Design or early Prototypes
  - File catalogue and SE synchronization
  - EMI Service Registry
- Production ready (on top of EMI-0)
  - GLUE2 support in compute area

EMI phase 2 (2012 April)

- Consolidation plans
  - Security area components
  - Information system components
- Design or early Prototypes
  - EMI_authlib
  - EMI_datalib
  - Messaging-based service instrumentation
- Production ready (on top of EMI-1)
  - CEs and clients with EMI interface
  - CEs with EMI accounting record
  - Consolidated compute area CLIs and APIs
  - GLUE2 support in data area
  - Glue2 support in infra area
  - All SEs supporting ”file://”, https, WebDav
  - Adoption of a fully consistent SRM implementation within data area
  - SEs and LFC synchronization
  - Transparent integration with AAI
  - VOMS as the single common EMI Attribute Authority Service
  - ARGUS and compute area services integration
  - EMI Service Registry
  - Messaging-based accounting publishers for compute and data area
  - Messaging-based monitoring sensors for all EMI services

EMI phase 3 (2013 April)

- Production ready (on top of EMI-2)
  - CEs capable scaling out to Clouds
  - CEs with consolidated MPI support
  - Consolidated data components including migration to EMI_datalib
  - Complete support for storage space accounting
  - Consolidated information system components
  - Consolidated security area components including migration to EMI_authlib
  - ARGUS and data area services integration
  - ”Cloud-friendly” EMI services

References

- EMI Technical Development plan (DNA1.3.1)
- Technical area workplans
  - Compute area work plan and status report (DJRA1.1.2)
  - Data area work plan and status report (DJRA1.2.1)
  - Security area work plan and status report (DJRA1.3.1)
  - Infrastructure area work plan and status report (DJRA1.4.1)
- Development plans for EMI 1
- Software Release plan (DSA1.2)

All documents are now in the project internal review phase and will be publicly released before the end of November

Thank you

EMI is partially funded by the European Commission under Grant Agreement INFSO-RI-261611