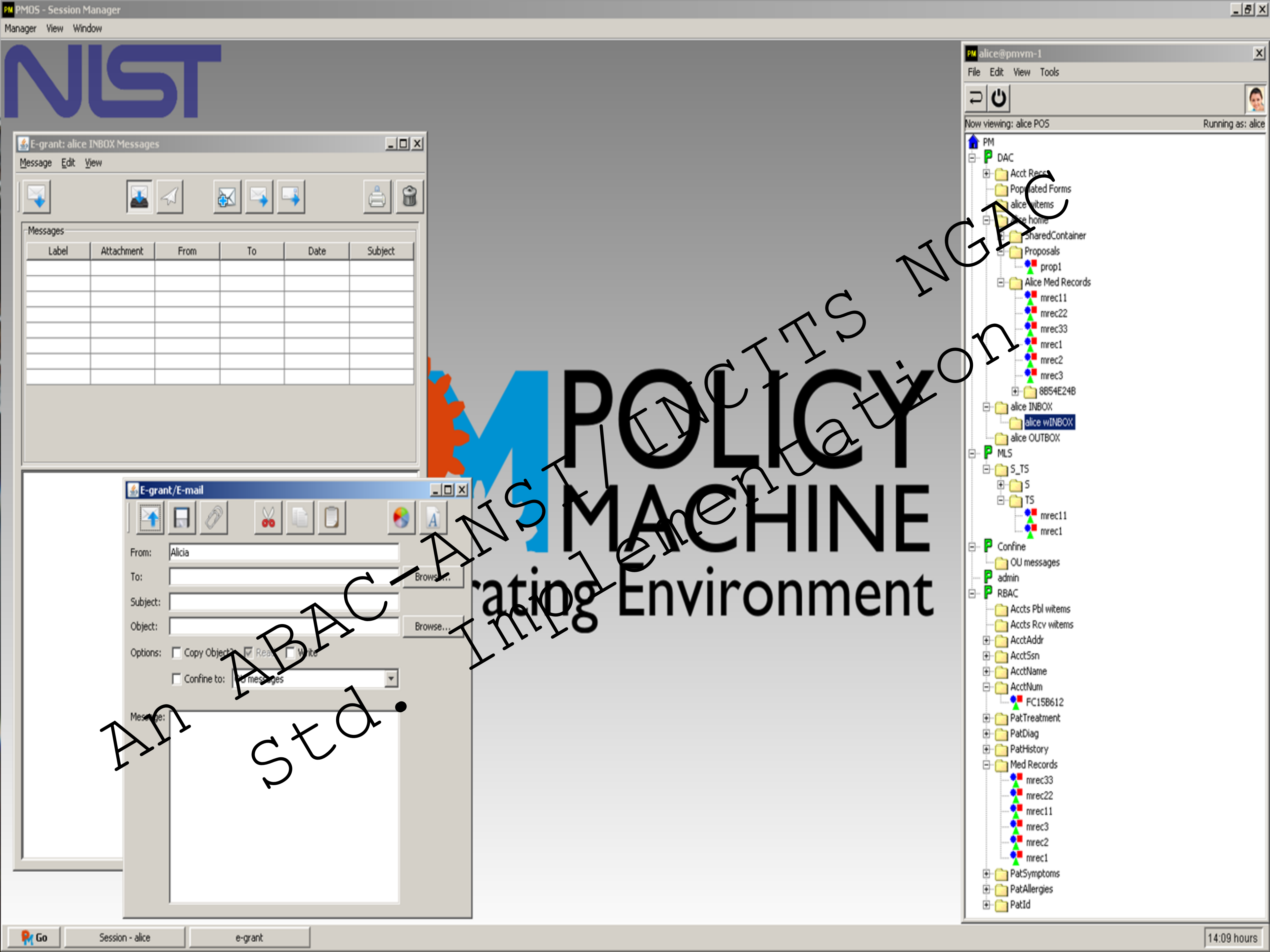
File-Sharing through NGAC*/ABAC for Secure Collaboration

David Ferraiolo, Serban Gavrila,
Gopi Katwala
National Institute of Standards and Technology

* Next Generation Access Control is an emerging ANSI/INCITS standard



An ABAC-ANSI/INCITS NGAC Std. Implementation

PMOS - Session Manager

Manager View Window

E-grant: alice INBOX Messages

Message Edit View

Messages

Label	Attachment	From	To	Date	Subject

E-grant/E-mail

From: Alicia

To:

Subject:

Object:

Options: □ Copy Object ☑ Read □ Write

□ Confine to: OU messages

Message:

alice@pmvm-1

File Edit View Tools

Now viewing: alice POS

Running as: alice

```
PM
  DAC
    Acct Recs
    Populated Forms
    alice witems
    alice home
      SharedContainer
      Proposals
        prop1
      Alice Med Records
        mrec11
        mrec22
        mrec33
        mrec1
        mrec2
        mrec3
        8B54E24B
    alice INBOX
      alice wINBOX
    alice OUTBOX
  MLS
    S_TS
      S
      TS
        mrec11
        mrec1
  Confine
    OU messages
  admin
  RBAC
    Accts Pbl witems
    Accts Rcv witems
    AcctAddr
    AcctSsn
    AcctName
    AcctNum
      FC15B612
    PatTreatment
    PatDiag
    PatHistory
    Med Records
      mrec33
      mrec22
      mrec11
      mrec3
      mrec2
      mrec1
    PatSymptoms
    PatAllergies
    PatId
```

Innovation

- Access Control and a Data Service Operating Environment can be built from the same underlying elements

Natural Consequences:

- Data service logic implemented through access control
- Data interoperability among data services
- Comprehensive policy enforcement across data services
- Users can see and consume all their authorized data under a single authenticated session

***** Data Services are both applications and system utilities that consume, manipulate, manage, and share data.

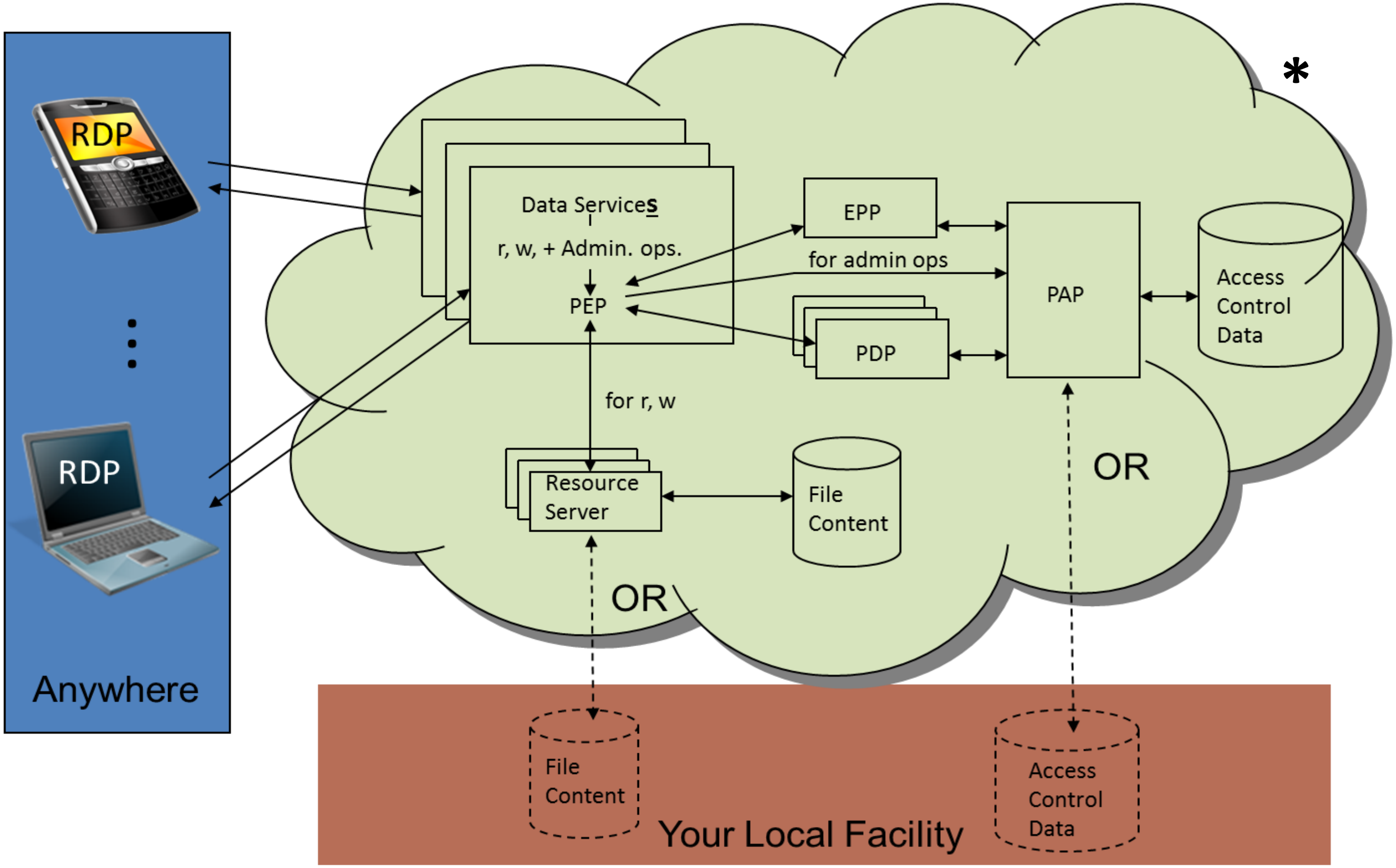
Other Features

- Policy preserving, file-sharing through data services
- All objects are files, but often perceived as other data types, (e.g., messages, work items, records, clip-board)
- Data never moves and only appears to be in application structures (e.g., folders, inboxes, columns).
- Share one file or data in bulk
- Users access files, and manage policies and attributes through the same PEP interface

Operating Environment

- **Data Services**: Office applications, file management, e-mail, workflow, records management, cut/copy-paste
- **Policies:** Tailored combinations of discretionary, mandatory, confinement, and history based access controls:
  - DAC
  - RBAC
  - Communities of Interest
  - Separation of Duty
  - Conflict of Interest
  - Forms of confinement (read with restrictive write)
    - E.g., Only doctors can read medical records & MLS
    - Trojan resistant leakage
  - Read once, give exclusive read away
  - Non-repudiation
  - Tracking access - I know who can currently access to my data

Cloud-like Deployment



* ANSI/INCITS NGAC Compliant

Status

- Version 1.0 on GitHub and version 2.0 coming in the spring of 2016.
- ANSI/INCITS NGAC - Generic Operations and Data Structures has been approved and NGAC Functional Architecture is a national standard.
- CRADA Opportunities
  - Let’s Collaborate: The difference is yours