IAM Task Force Update

April 3, 2015

For Today

- The Group
- The Charge
- IAM at CSU
- Recommendations
- Discussion

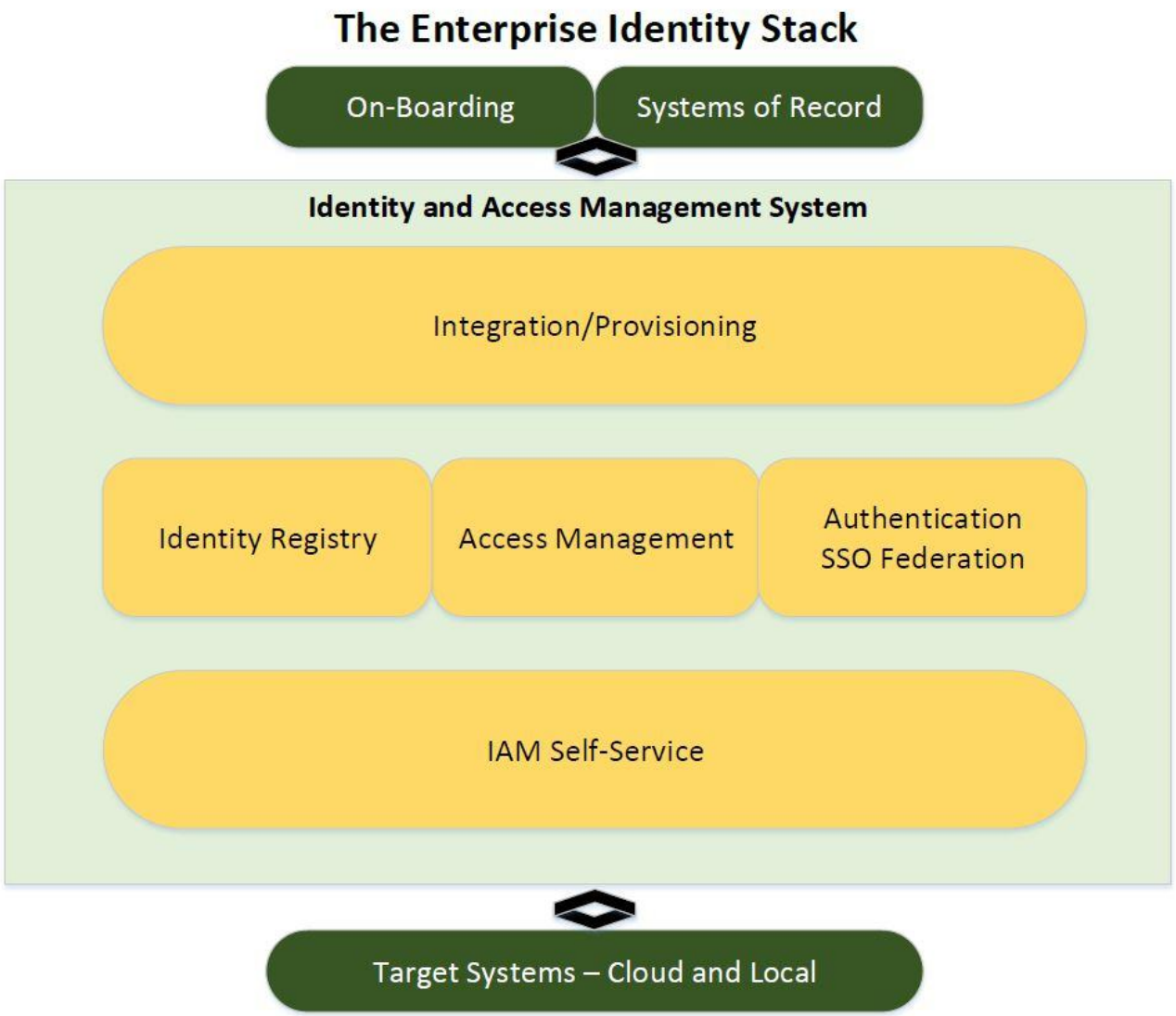
Task Force Members

- Human Resources – Tracy Hutton
- College IT Administrators Council
  - Scott Novogoratz – CVMBS
  - Dave Carpenter – CHHS
- Research Services – Ron Splittgerber
- Information Systems – Bob Engmark
- Internal Auditing – Stephanie Wolvington
- ACNS (Middleware) – Randy Miotke
- Chair, Rusty Scott

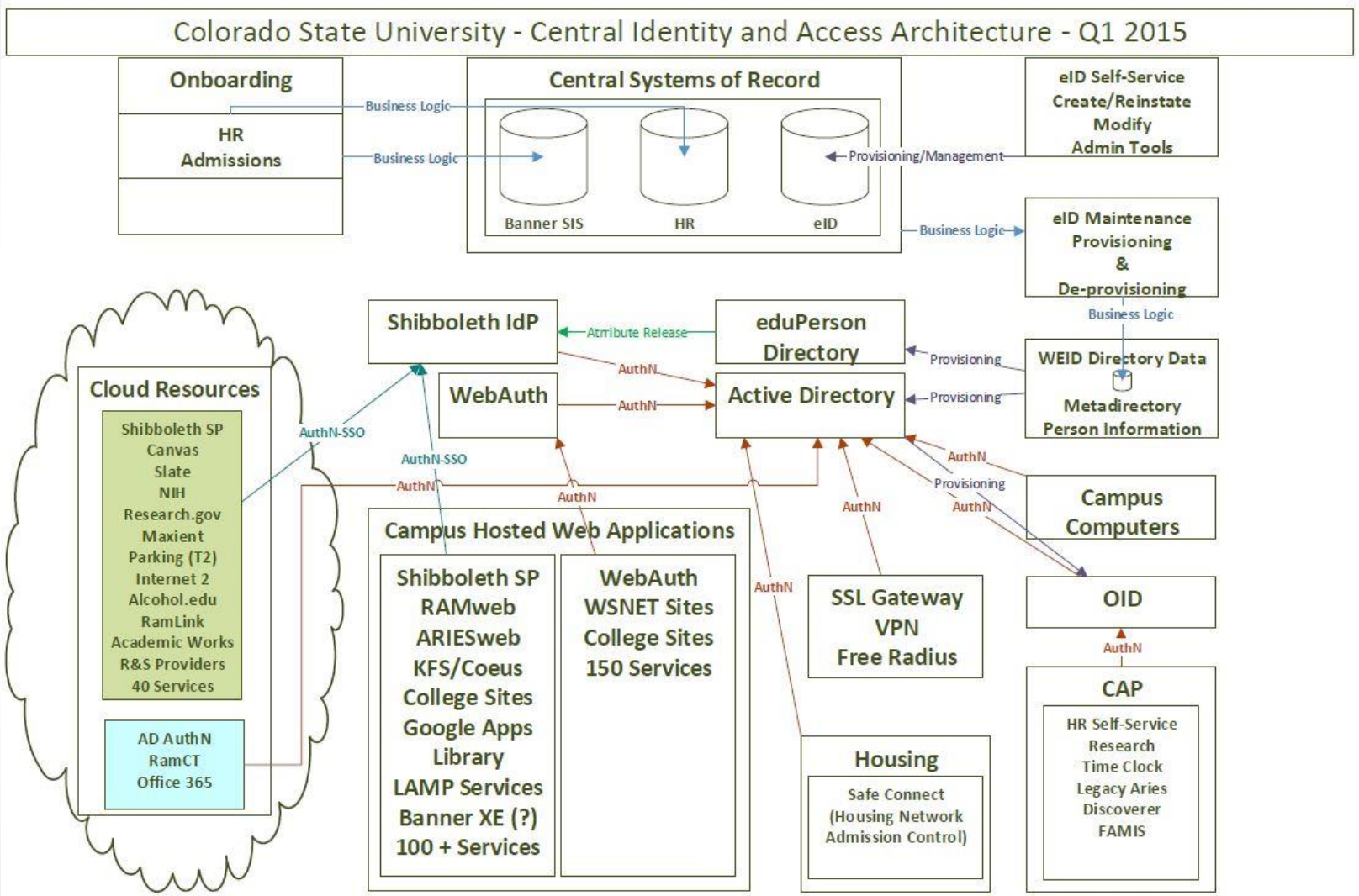
The Charge – Salient Points

- Strategic rather than operational
  - Operational efforts will spin from this as approved by IAC
- Will need to remain somewhat agile to act ‘consultative’
- Provide roadmap for IAM that is modern, scalable, manageable and functional with a particular focus on:
  - Simplifying the environment
  - Improving services for both internal and external users

IAM Components



CSU's IAM Ecosystem



General Recommendations

1) Establish a central authorization process for providing access to CSU's systems & services
2) eIDs should persist
    1) As a rule, discontinue the notion of active/inactive identities
    2) Leverage authorization for managing access to services
3) Seek alternative for managing credentials for external (non-eID) users
    1) Big problem that is only getting bigger
4) Continue to simplify the environment
    1) For everyone – End Users, architecturally
5) Codify Bronze level assurance for CSU, silver as soon as possible

More Specifically…

Authorization Services

- For effective, flexible role-based access management for groups and individuals
- For better, policy-based de-provisioning of services
- Should include delegated administration
- Currently missing from our IAM environment
- Recommendation:
  - Explore feasibility and scope of implementation
    - E.g., Kuali, Banner, HR

Persistent eIDs

- Preserve identities for those with formal relationship with CSU
  - Wins for Alumni Association, Advancement, RamRecords, others
  - Returnees are granted access to services as needed
- Align with out current “de minimis access” model
- Dependent on central authorization services
- Recommendation:
  - After authorization services are in place, discontinue practice of deactivating identities

External (non-eID) Users

- Many in-house credentialing systems in existence today
- Opportunity to off-load this to external services
  - Google, Facebook, others
- Does not address authorization but could be a significant step in simplification
- Recommendation:
  - Identify suitable pilot population and service
  - Engage with Cirrus Identity for 'Social-to-SAML' for gateway services

Simplifying the Environment

- Recommendation: Reduce the number of child domains
  - Results in fewer credential pairs for users
  - Complete elimination is likely too extreme
    - Effective for managing (authorizing) resources in complex domains
  - Authorization services would enable smoother transition
  - Develop policies/guidelines for when child domains are appropriate
- Recommendation: Move to a single authentication technology, Shibboleth
  - WebAuth
    - Long & successful history
  - Shib
    - Standard across institutions, enabling federation
    - True Single Sign-On
    - Today, 40 external services, 110 on-campus services
- For both, transition roadmap, help and training to be provided centrally

InCommon Level of Assurance
- Address of Record Confirmation Compliance

- Item 4.2.2.5 states that we need to verify the Address of Record
- Email is much more efficient and effective than physical address
- Requires a slight modification to eID 'create' process
  - Send one-time expiring token & link to the user's email address on record
  - Would enable pre-population of basic info needed for eID creation
    - Avoids confusion related to format of birthdate, complex last names
  - Consistent process for all users (students, employees, associates)
- Recommendation:
  - Implement Address of Record confirmation process into the eID create process
  - Timeline: Summer 2015, contingent upon approval of stakeholders (Admissions, HR, Grad School)

Assurance, cont'

- Silver is still the goal, architectural & training hurdles still remain
- Regarding Bronze:
  - Not a huge functional win today
  - Really good PR internally and with the Feds
    - Evidence that we are doing things right with respect to federal and InCommon security and compliance guidelines
      - Protection of PII
      - Credential creation, revocation requirements
      - Authentication and encryption technologies are sound
      - Record keeping
- Recommendation:
  - Do not let up on pursuing Silver level Assurance
    - Explore AD encryption, 2-factor authentication
  - Apply for Bronze once Lamar is decommissioned
  - FYI today, 5 institutions bronze, one silver

Other Conversations - TIER

- Trust and Identity in Education and Research
- Internet 2 initiative aiming to:
  - Provide federated identity, attribute and authorization management
  - Leverage prior efforts
  - Accelerate adoption
  - Integrate existing components
  - Sustain development and support plan
- Recommendation:
  - Follow effort, for now
  - Current CSU initiatives tracking pretty closely

Discussion

- Most consistent thread in our conversations to date:
  - Authorization process/services
- In general, are we heading the right direction?