EGI Updates
Check-in

Matthew Viljoen – EGI Foundation
Nicolas Liampotis – GRNET
Peter Solagna – EGI Foundation

FIM4R, 19 Sept 2017, Montreal
Contents

• Overview
• Use cases
• Production status
• Work in progress
Check-in Overview
Check-in provides a reliable and interoperable AAI solution for the EGI service providers federation, and external service providers. It enables single sign-on to services through eduGAIN identity providers and other institutional or social media credentials.

- Check-in development, lead by GRNET, has been supported by the EGI-Engage project. The EGI Council supports the long-term operations of the service.
- Check-in has been developed in close collaboration with the AARC project, and it implements the recommendations of the AARC Blueprint Architecture and Policy Framework.
Check-in Features

• Supports **authorised access to protected resources** based on VO/group membership and role information
• **Aggregates** user attributes from different sources, including external community-managed attribute providers
• Supports the **linking** of multiple external identities to a persistent, non-re-assignable, unique user identifier within the EGI infrastructure
• Associates a **Level of Assurance** (LoA) to each authenticated identity in the EGI infrastructure
• **Reliable and secure:** Highly available by design. Operated under the strict security policies of the EGI federation, and the EGI Foundation ISO20k-certified processes
• **Simple:** CheckIn hides the complexity of dealing with multiple IdPs and sources of authorisation information
• **Low overhead:** Service providers do not need to deal with the bureaucracy of integrating with multiple identity providers and attribute authorities
• **Interoperable:** Published in eduGAIN as a service provider compliant with REFEDS R&S and Sirtfi. Supports translation of credentials across the most popular standards: SAML 2.0, OpenID Connect, OAuth 2.0, and X.509
Check-in Architecture

- Implementation of the AARC blueprint architecture
- All EGI SPs can have one statically configured IdP
- No need to run an IdP Discovery Service on each SP
- Connected SPs get consistent/harmonised user identifiers and accompanying attribute sets from different IdPs/AAs that can be interpreted in a uniform way for authorisation purposes
- External IdPs only deal with a single EGI SP proxy
Check-in use cases
Community operating its own AAI connected as an IdP to CheckIn to allow its users to access EGI services & resources

✔ Access EGI services without changing your authentication workflow
Community managing authorisation information about the users (VO/group memberships and roles) via their own group management service, which is connected to Check-in as an external attribute authority

- Check-in will handle the configuration of the IdPs and the aggregation of the attributes for the SPs
- No need to migrate the group management functionality to an EGI-specific attribute authority
For the communities: full AAI platform with group management as a service

Communities that do not operate their own group management service can leverage the group management capabilities of the CheckIn platform

- Ready-to-use solution
- Avoid overhead of deploying a dedicated group management service
- Support for multi-tenancy to allow authorised VO admins to manage the information about their users independently
- Easy connect to both EGI and non-EGI services
For service providers: AAI as a service

Check-in as an authentication proxy

✓ Enable login from institutional IdPs in eduGAIN and social media

✓ Minimal overhead for the service development

✓ All the other CheckIn features are available for the SP: account linking, attribute aggregation, ..

• Prerequisites:
  ✓ Service provider must accept EGI policies on data protection
Check-in production status
Check-in today

- **Identity Providers:**
  - SAML2.0: eduGAIN
  - OIDC/OAuth2: Google, Facebook, LinkedIn, ORCID
  - X.509: IGTF

- **Service Providers:**
  - SAML2.0 & OIDC

- **Attribute Authorities**
  - SAML2.0 Attr. Query, REST, LDAP, SQL

- **Token Translation Services**
  - SAML2.0-to-X.509: Master Portal to RCauth.eu Online CA

- **Support for Levels of Assurance**
- User enrolment & account linking
- IdP Discovery
- User Consent
Check-in consumes information from many diverse sources

CheckIn

- COmanage
- Perun
- SAML IdP
- OpenID Connect IdP
- VOMS
- GOCDB
- e/R-Infra AAI proxy (e.g. ELIXIR)
- External VO Management (e.g. Unity IDM)
Support for Levels of Assurance

- Check-in supports 3 different Levels of Assurance:

<table>
<thead>
<tr>
<th>Key features/Profiles</th>
<th>AARC-Assam</th>
<th>IGTF-DOGWOOD</th>
<th>IGTF-BIRCH</th>
<th>AARC-Darjeeling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique ID</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Identity Vetting</td>
<td></td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Multi Factor</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

- Use case
  - Check-in conveys the LoA associated with the authenticated identity to SPs for authorisation purposes
    - Communicated through the eduPersonAssurance attribute in SAML or acr claim in OIDC
    - Translated into entitlements expressing the right of a user to access a particular resource (e.g. access Rcauth Online CA)
Check-in will implement the AARC guidelines to express group membership information

Use of URN-formatted entitlement values:

<namespace>:group:<group>[::<subgroup>]*[::<role>=<role>]#<group-authority>

• <group> is the name of a VO, research collaboration or a top level arbitrary group; unique within a given <namespace>
• optional list of <subgroup> components represents the hierarchy of subgroups in the <group>
• optional <role> component indicates particular position of the user; scoped to the rightmost (sub)group
• <group-authority> indicates the authoritative source for the group membership and role information
User-friendly interface for managing OpenID Connect/OAuth 2.0 tokens

• Provides users with an overview of all OpenID Connect/OAuth 2.0 services they have authorised to access their EGI account
• Allows users to see the specific permissions (e.g. read email, offline access, etc.) granted to each service
• Enables users to manage access/refresh tokens associated with each service:
  – Revoke access for individual tokens or service as a whole
  – Retrieve access/refresh tokens to be used for federated access to CLI tools/APIs
• Check-in has been integrated with the production RCAuth.eu Online CA
  – Users can retrieve X.509 proxies by authenticating through Check-in
Reliable and secure AAI platform

EGI has always invested in improving and maintaining the reliability and security of the services

- EGI has a mature and complete set of security policies and the processes to enforce them
  - Extended with Check-in specific policies:
    ✓ Check-in acceptable usage policy
    ✓ Check-in data protection policy
    ✓ Agreement documents to integrate non-EGI and non-eduGAIN SPs and IdPs and maintain the compliance
Work in progress
Check-in Next Steps

- Align with AARC guidelines on expressing group membership and role information
- Align with REFEDS/AARC Assurance Profiles
- Complete integration with EUDAT AAI
- Provide user-friendly interfaces for managing OpenID Connect/OAuth 2.0 tokens
- Support for (de-)provisioning and continuous update of user account information
Thank you for your attention.

Questions?