Insperity + Workday + BrightMove SSO Integration

Solution Design Document

Project: Insperity + Workday + BrightMove SSO Integration

Date: July 24, 2025

Version: 1.1

Prepared by: BrightMove Solutions Team

Executive Summary

This solution design provides a comprehensive approach for enabling SAML-based Single Sign-On (SSO) integration between Insperity Premier, Workday, and BrightMove ATS. The solution ensures both the legacy Premier SSO and the new Workday SSO can coexist, with BrightMove ATS adapting to assertion differences and security requirements. The project is targeted for completion within 1 month and a budget of $2,000, contingent on stakeholder acceptance and support for testing.

1. Project Stakeholders

Insperity Team

- **Karen Millard** - ITC Product Manager
- **Martha Vera** - ITC Product Owner
- **Kaysie McCormick** - Enterprise Project Manager
- **Eugene Chang** - Workday Solution Architect

BrightMove Team

- **Jimmy Hurff** - Head of Customer Success
- **David Webb** - CEO & Head of Product

2. System Components Architecture

Insperity Systems

- **ITC (Insperity Talent Connect)** - White-label BrightMove ATS platform branded for Insperity customers
- **Workato** - Insperity-managed iPaaS integration platform
- **Workday** - Insperity-managed ERP platform
- **Premier** - Insperity-managed customer-facing portal

BrightMove Systems

- **ATS (Applicant Tracking System)** - Multi-tenant, AWS-hosted platform for Insperity customers

3. Problem Statement

Challenge: Insperity is migrating to Workday and requires SSO integration for both Premier (legacy) and Workday (new) platforms with BrightMove ATS. Both SSO solutions must coexist, with no adverse impact on the current Premier SSO. BrightMove ATS must handle assertion differences and encryption limitations between the two SSO sources.

- The current SSO solution connects Insperity Premier using SAML (since 2011).
- The new Workday platform needs to be integrated with ATS via SSO.
- Both integrations must run concurrently and securely.
- Premier SSO assertions include AIMS ID and Company GK; Workday SSO will only send userGK.
- Workday SSO assertions will not be PGP encrypted; Premier assertions may be encrypted.

Business Impact

- **Seamless User Experience:** Users can access BrightMove ATS from both Premier and Workday without disruption.
- **Security:** SAML assertions and key management must meet Insperity and BrightMove security standards.
- **Business Continuity:** No downtime or loss of access for Insperity users during migration.

4. Solution Architecture

SAML SSO Integration

Overview: Both Premier and Workday will use SAML-based SSO to authenticate users into BrightMove ATS. SAML assertions will include required attributes and be signed/encrypted according to best practices. BrightMove ATS will adapt to assertion differences and encryption limitations.

```
┌───────────────┐    ┌───────────────┐    ┌───────────────┐
│  Premier      │    │  Workday      │    │ BrightMove    │
│  (SAML SSO)   │    │ (SAML SSO)    │    │     ATS       │
└─────┬────────┘    └─────┬────────┘    └─────┬──────────┘
      │                     │                   │
      └─────────────┬───────┴───────────────┬──┘
                    │   SAML Assertion      │
                    │  (userGK, [AIMS ID, Company GK - Premier only]) │
                    │   [Encrypted - Premier only] │
                    └─────────────┬─────────┘
                                  │
                        [SAML Endpoint]
               http://app.brightmove.com/ATS/app/auth/saml
```

Attribute Mapping & Assertion Handling

- **userGK:** BrightMove unique user ID (required for both Premier and Workday SSO)
- **AIMS ID, Company GK:** Present in Premier SSO only; ATS must handle their absence in Workday SSO
- **Encryption:** Premier SSO assertions may be encrypted; Workday SSO assertions will not be encrypted

Security and Key Management

- SAML assertions will be signed with Insperity/Workday private key and encrypted with BrightMove public key (where supported)
- X509 certificates will be exchanged via secure channels (SFTP, email)

- ATS must validate and process both encrypted and unencrypted assertions

5. Functional Requirements

FR-001: Dual SSO Support

Requirement: Support SAML SSO from both Premier and Workday into BrightMove ATS, with concurrent operation.

Acceptance Criteria: Both SSO integrations function concurrently without conflict.

FR-002: Assertion Adaptation

Requirement: ATS must handle SAML assertions with and without AIMS ID, Company GK, and encryption.

Acceptance Criteria: Users from both Premier and Workday can authenticate successfully; missing fields do not cause errors.

FR-003: Attribute Mapping

Requirement: Map Workday Employee ID to BrightMove userGK for SSO.

Acceptance Criteria: SAML assertion includes correct mapping and required attributes.

FR-004: SAML Assertion Validation

Requirement: Validate SAML assertions, signatures, and decryption using exchanged keys (where applicable).

Acceptance Criteria: Only valid, signed, and properly encrypted (if present) assertions are accepted.

FR-005: Backward Compatibility

Requirement: Maintain backward compatibility with existing Premier SSO.

Acceptance Criteria: No adverse impact on current SSO users.

FR-006: Endpoint Availability

Requirement: Provide SAML assertion consumption endpoints for QA and Production.

Acceptance Criteria: Endpoints are available and documented for both environments.

6. Non-Functional Requirements

NFR-001: Security

- All SAML assertions must be signed; encryption applied where supported.
- Key management must follow Insperity and BrightMove security policies.

NFR-002: Performance

- SSO authentication should complete within 2 seconds.

NFR-003: Reliability

- 99.9% uptime for SSO endpoints.

NFR-004: Compliance

- Adhere to all relevant data privacy and security standards.

NFR-005: Testing

- Support both QA and production environments for integration and validation.
- Testing support from Workday and Insperity is required for validation.

7. Project Timeline and Milestones

1-Month Implementation Schedule

Week 1: Planning & Design

- Requirements validation and technical design
- Key and certificate exchange

Week 2: Development

- Implement SAML assertion handling and attribute mapping
- Develop and test SSO endpoints

Week 3: Integration & Testing

- Integration testing with Premier and Workday
- Security and performance validation

Week 4: Deployment & Go-Live

- Production deployment
- Stakeholder review and sign-off

Key Milestones

- **Week 1:** Technical architecture approved, keys exchanged
- **Week 2:** SSO endpoints and attribute mapping implemented
- **Week 3:** Integration and security testing complete
- **Week 4:** Go-live and project completion

8. Resource and Infrastructure Requirements

BrightMove Team

- 1 Developer (0.25 FTE for 1 month)

Insperity Team

- 1 Workday Integration Developer (0.25 FTE for 1 month)

Infrastructure Requirements

BrightMove Infrastructure

- Existing SAML endpoint infrastructure
- Monitoring and logging tools

Insperity Infrastructure

- Workday and Premier SSO configuration
- Certificate/key management

9. Cost Estimation

Resource	Duration	Cost
BrightMove Developer (0.25 FTE)	1 month	$2,000
Total Project Cost		**$2,000**

10. Risk Assessment and Mitigation

Risk 1: SSO Coexistence

Probability: Medium

Impact: High

Mitigation: Careful testing and validation of both SSO integrations before go-live.

Risk 2: Assertion Differences

Probability: Low

Impact: Medium

Mitigation: ATS logic to handle missing/encrypted fields and assertion variations.

Risk 3: Key Management Issues

Probability: Medium

Impact: Medium

Mitigation: Use secure channels for key exchange and follow best practices for certificate management.

Risk 4: Timeline Compression

Probability: Medium

Impact: Medium

Mitigation: Focused scope, agile development, and early stakeholder engagement.

11. Success Metrics and KPIs

SSO Reliability

99.9%

Target: SSO endpoints available and functional

Success Criteria: No unplanned downtime

Security Compliance

100%

Target: All assertions signed/encrypted as required

Success Criteria: No security incidents

User Experience

Seamless

Target: Users access ATS from both platforms without issue

Success Criteria: No user complaints or access issues

12. Monitoring and Maintenance

Monitoring

- SSO endpoint uptime and error tracking
- Key/certificate expiration monitoring

Maintenance

- Key/certificate rotation as required
- Periodic security reviews

13. Next Steps and Statement of Work

1. **Stakeholder Approval:** Obtain formal approval from designated stakeholders
2. **Key Exchange:** Complete secure exchange of certificates/keys
3. **Development:** Implement and test SSO integrations
4. **Go-Live:** Deploy to production and monitor

Statement of Work Development

Upon approval of this solution design, a detailed Statement of Work (SOW) will be prepared outlining deliverables, timeline, and acceptance criteria.

Approval Process

This solution design requires formal approval from:

- **Insperity:** Karen Millard (ITC Product Manager), Martha Vera (ITC Product Owner), Kaysie McCormick (Enterprise Project Manager), Eugene Chang (Workday Solution Architect)
- **BrightMove:** Jimmy Hurff (Head of Customer Success), David Webb (CEO & Head of Product)

14. Conclusion

This SSO solution design enables secure, seamless authentication for Insperity users across both Premier and Workday platforms, ensuring business continuity and security. Upon approval, the project will proceed to Statement of Work and implementation phases.

Document Control

Version: 1.1

Last Updated: July 24, 2025

Next Review: Upon stakeholder approval

Distribution: All project stakeholders

Approval Status: Pending formal approval from designated stakeholders before proceeding to Statement of Work development.