

UI Identity (ID) Proofing Services and Solutions Recommended Contract Provisions

In evaluating potential service providers to deliver a solution for ID proofing, states should consider including the following recommended contract provisions.

Recommended Technical Provisions

1. Digital ID Proofing
2. Data Privacy & Sharing
3. Data Access & Ownership
4. Audit Trail
5. Performance, Scalability & Availability
6. Support & Training
7. Service Level Provisions
8. General Provisions – Section 508 Compliance

Recommended Business Provisions

1. Business Performance Provisions (Timeliness and Transparency)
2. Equity Provisions

More detail on each recommended provision, including the specific recommendation, its purpose, and the sample contract language is included in the table below.

Digital ID Proofing		
Recommended Provision	Purpose	Sample Contract Language
<p>Implement ID proofing that balances equitable access with alignment to National Institute of Standards and Technology’s (NIST)’s digital identity guidelines. (See https://csrc.nist.gov/publications/detail/sp/800-63a/final). Section 4.4 pages 8-11.</p> <p>CAUTION: Carefully review solutions that use biometrics such as facial recognition. While these solutions may help to reduce identity fraud, they may have negative implications for equity or lead to violations of states’ nondiscrimination obligations under Section 188 of Workforce Innovation and Opportunity Act (WIOA).</p>	<p>Improves speed of delivery of benefit payments by establishing high confidence in the claimant’s identity. Reduces workload on state staff by assisting on identity verification. Reduces online fraud, including identity theft and identity fraud.</p>	<ul style="list-style-type: none"> • Solution incorporates best practices from NIST 800-63-3 guidelines while ensuring equitable access. • Solution provides configurable and accessible User Interfaces/User Experience (UX) flow that is mobile-responsive and compatible with multiple browsers and device types as per industry standards. • Solution provides verified, not verified, and pending outcomes along with configurable data associated back to calling systems for continuation of adjudication and processing of claims or other related activities.
<p>Implement authentication to online systems incorporating best practices from NIST’s Authenticator Assurance Level (AAL) 2 standard definition. (See https://csrc.nist.gov/publications/detail/sp/800-63b/final). Section 4.2 pages 6-8.</p> <p>CAUTION: NIST 800-63-3 AAL2 recommends very strict session timeouts that may be burdensome to some applicants, particularly to those less familiar with multi-factor authentication. States are encouraged to balance these factors and exercise judgment when instituting secure authentication.</p>	<p>Reduces fraud and online “claims hijacking” also known as “claims or account takeover” by establishing stronger authentication/verification of the claimant’s online identities when accessing systems to change contact information, address information, and bank account information.</p>	<ul style="list-style-type: none"> • Solution incorporates best practices from the NIST 800-63-3 AAL2 standard. • Solution provides configurable and accessible User Interfaces/UX flow that is mobile-responsive and compatible with multiple browsers and device types as per industry standards.

Data Privacy and Sharing		
Recommended Provision	Purpose	Sample Contract Language
Require Data Privacy & Data Sharing Provisions.	Protects user data from unauthorized disclosure, particularly Personally Identifiable Information (PII) and sensitive information.	<ul style="list-style-type: none"> • Disclose all uses of user data including data sharing with third parties and how they mitigate potential third-party service bad actors or negligent actors to ensure the protection of user data, especially PII and sensitive information. • Support supply chain audits as requested by state and must comply with the provisions of the Privacy Act of 1974. All personnel assigned to this contract are required to take proper precautions to protect the information from disclosure. The contractor must not release, publish, or disclose sensitive information to unauthorized personnel, and must protect such information following provisions of the following laws and any other pertinent laws and regulations governing the confidentiality of sensitive information: 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records).
Prohibit Claimant Data Resale or Commercial Use.	To prevent the resale or commercial use of claimant or state data.	<ul style="list-style-type: none"> • Prohibition on Claimant Data Resale or Commercial Use: The contractor is prohibited from reselling or using for any commercial purpose, whether individually or in aggregate, any claimant or state data collected in the execution of the contract or subsequent orders. Sharing of data other than for the express purpose of identity verification for Unemployment Compensation (UC) claims is strictly prohibited.

Data Access & Ownership		
Recommended Provision	Purpose	Sample Contract Language
Preserve State Access to and Ownership of Government Data.	To preserve a state's ability to create, maintain, and modify the Government Data included within the solution.	<p>At a minimum, the solution must support the following Data ownership requirements inclusive and not limited to:</p> <ul style="list-style-type: none"> • Machine-Readable Exports: Solution must support creating a digital, reusable copy of the Government Data, in whole and parts, as a platform-independent and machine-readable file. • Use of Government Data: Solution's copyright, patent, or intellectual property considerations must not restrict state use of the solution to create, maintain, and modify the Government Data. The solution must not make use of the Government Data for any commercial purpose or any purpose not specified in this agreement, whether to the benefit of the solution's vendor or a third-party.

Audit Trail		
Recommended Provision	Purpose	Sample Contract Language
Provide a comprehensive audit trail (<i>See: NIST SP 800-53 Rev 5.0</i>).	The selected vendor must provide a thorough and comprehensive audit trail. It is important to have a full accounting of who applied for benefits, what the decision was, etc. This will assist with required compliance reporting, as well as provide documentation on state decisions should the state face legal challenges.	<ul style="list-style-type: none"> Audit reports must have comprehensive audit trail capability to collectively provide documentary evidence of the processing used to aid in tracing from original transactions forward to related records and reports, and/or backwards from records and reports to their component source transactions. The Audit trail must comply with NIST SP 800-53 Rev 5.0 controls contained in the Audit and Accountability family. The solution must provide reporting for compliance with the Federal Information Security Modernization Act of 2014 (FISMA) and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (as amended).

Performance, Scalability & Availability		
Recommended Provision	Purpose	Sample Contract Language
Ensure system's capability to scale up quickly and effectively to handle increased caseloads.	It is crucial that the supplied solution be able to scale up quickly and efficiently, should there be a surge in UI claims, so that response time and throughput are not negatively impacted.	<ul style="list-style-type: none"> System's capability to handle an increasing number of users or an increase in requests (<i>e.g.</i>, more than 500,000 ID proofing requests per week) without adversely affecting response time and throughput. The uptime guarantee for production instances must be 99.95% to prevent the impact on the UI programs.

Support & Training		
Recommended Provision	Purpose	Sample Contract Language
<p>Provide robust training and support network for both program staff and UI applicants.</p>	<p>The selected contractor must provide a robust training and support network to support both program staff and UI applicants.</p> <p>This training should include, at a minimum, an online repository of help guides and videos. Support should include, at a minimum, a call center to assist with login, ID proofing, and multi-factor authentication help desk tickets.</p>	<ul style="list-style-type: none"> • The contractor must provide customer support for state client bases, including, but not limited to, system owners and managers, as required. • Support state technical staff to create stable integration architecture. • Call center support for all login, ID proofing, Multi-Factor Authentication (MFA) help desk tickets. • Support for individuals whose ID proofing is pending or is in failed status while attempting to obtain verification. • Provide prioritized integration/implementation, architecture, and solutions support. • Training support such as conducting webinars, online videos, and other documentations as needed. • Online technical and user documentation (architecture, help guides, videos, runbooks, etc.).

Service Level		
Recommended Provision	Purpose	Sample Contract Language
<p>Provide rapid response times for ID verification.</p>	<p>The selected contractor should prioritize rapid response times for ID verification. The target should be to provide a decision for supervised remote ID verification in no more than 48 hours and for unsupervised ID verification in no more than 5 minutes. Likewise, average page load times should not exceed 5 seconds. This will ensure customer satisfaction and an efficient and effective ID verification process.</p>	<p>In additional general service/support activities, the contractor must comply with the following:</p> <ul style="list-style-type: none"> • Supervised remote ID verification must not exceed 48 Hrs. to provide a decision outcome. • Unsupervised ID verification must not exceed 5 minutes to provide a decision outcome. • Average response times for page loads must not exceed 5 seconds. • Priority 1 helpdesk and product/technical support tickets must be processed in 2 Hrs. Priority 2 product/technical support tickets must be processed in 24 Hrs. All other product/technical support tickets must be processed within a 72 Hrs. • Authentication and ID verification error rates (false positives or false negatives) must not exceed 1%

General		
Recommended Provision	Purpose	Sample Contract Language
Meet state-specific security and Section 508 Compliance standards.	To ensure that the content is accessible to people with disabilities.	<ul style="list-style-type: none"> • The selected contractor must ensure compliance with state-specific security standards as well as Section 508 of the Rehabilitation Act, to ensure that the content is accessible to people with disabilities. • The Section 508 standards incorporate by reference the Web Content Accessibility Guidelines developed by the Web Accessibility Initiative to make web pages as accessible as possible to the widest range of users, including users with disabilities.

Business Performance		
Recommended Provision	Purpose	Sample Contract Language
Timely communication of ID verification decisions to the state UI agency.	Timeliness and transparency are important pieces of the contractor's ID verification system. It is important to ensure that the contractor's ID verification system communicates the decision made on an individual's identity (<i>e.g.</i> , verified, not verified, pending) to the state UI agency. These decisions should be communicated in real-time, if possible, but no later than 24 hours after the individual begins the ID verification process. The contractor should also notify the individual of the decision within the same timeline discussed above.	<p>Timeliness:</p> <ul style="list-style-type: none"> • The contractor's ID verification system must be able to provide notification to the state UI agency whether an individual's identity has been verified, not verified, or is pending, if possible, in real-time, but no later than 24 hours after the individual started the ID verification/proofing process to the ID. • As requested by the state UI agency, contractor must notify the individual of whether their identity has been verified, not verified, or is pending, if possible, in real-time, but no later than 24 hours after the individual started the ID verification/proofing process.

Equity Provisions		
Recommended Provision	Purpose	Sample Contract Language
Ensure equitable access.	The contractor selected to provide ID verification services should have a plan to ensure equitable access to ID verification services, including for individuals with disabilities, individuals with Limited English Proficiency (LEP), older individuals, and those unable to access or use a web-based system. To ensure equity, the contractor should provide alternative access methods that are readily available, timely, and of no-cost to the individual.	<p>Unemployment Insurance Program Letter (UIPL) No. 02-16 (published October 1, 2015) and UIPL No. 02-16, Change 1 (published May 11, 2020), provide State Responsibilities for Ensuring Access to Unemployment Insurance Benefits, Services, and Information. Consistent with these requirements, the Department requires the contractor to provide the following.</p> <ul style="list-style-type: none"> • The contractor must provide an efficient alternative access method for individuals who are unable to complete ID verification through electronic or self-service means. This includes individuals with barriers to access, such as individuals with disabilities, LEP individuals, older individuals, individuals who experience challenges with technology, and individuals who experience challenges with literacy. This also includes individuals who need support troubleshooting. • The alternative access methods must: (1) ensure meaningful access to limited English proficient (LEP) individuals so that they are effectively informed about and/or able to participate in ID verification. Language assistance services must be accurate, provided in a timely manner, and free of charge to the individual; and (2) be advertised on the contractor’s application and include information about how an individual who has difficulty using the site or service can get assistance to access the site or service.