Contractor Enrollment and Onboarding

Whitepaper

Introduction

Driven by the need to enhance the security of digital transactions and to help protect customers' interests, the Reserve Bank of India (RBI) has issued a framework for alternative authentication mechanisms.

Identity and access management has gone essentially unchanged since the introduction of the password nearly 60 years ago. However, with the countless breaches happening, over 60% of those are due to a compromised credential - user name and password. So now, we see an inflection point where there is a push to eliminate passwords and move to passwordless authentication to solve the problem. The thought is, when moving to a passwordless model, an organization will eliminate the user name and password issue. But the truth is, passwordless authentication is still based on a user name and password. So really, the current approach is still based on the weakest link. To reach true passwordless authentication, organizations need to look beyond simply moving to a passwordless infrastructure and move to identity-based access control. This means bolstering authentication with an identity-proofed login so that administrators for the first time will know, with certainty, who is accessing corporate IT networks.

This differentiation will verify the user with identity-based biometrics at each access request, eliminate passwords, improve security and deliver a true passwordless experience. Internally there are likely measures in place to validate a new employee, but what about contractors? A new contractor rarely follows the same onboarding and enrollment as a new employee. And for that reason, whenever a contractor authenticates into the organization, there is no way of knowing that it is the contractor brought in or someone else working on their behalf.

As a result, organizations need to address three security issues:

1. The establishment of the username/password creates a vulnerability, as the manager and the admin both see the username/password before the contractor can reset
2. Securely enroll and onboard the contractor to a passwordless environment
3. Eliminate the potential contractor jacking

The 1Kosmos solution digitally transforms the standard HR process for onboarding employees or contractors, delivering the highest degree of end-user assurance. This transformation eliminates the need for new workers to share copies of government IDs, protects their privacy, and automates the onboarding process for new and existing contractors. By binding the contractor's proofed identity, 1Kosmos creates an identity-based biometric authentication and a passwordless experience. Contractors will utilize their trusted mobile device for daily authentication and step-up authentication for physical or logical access.

As a result, 1Kosmos eliminates what can be referred to as: ‘contractor jacking.’ When a contractor starts on day one, they may be the person you interviewed, but you have no idea who that is on day two. As a result, contractors have been known to sub out their seat to somebody cheaper and pocket the savings. And now, not only do you not get the person you hired, but you have extra security exposures because you didn’t do a background check on that person. So our approach to digital onboarding and enrollment of new contractors ensures each access event is associated with a real, verified identity, ensuring it’s the hired contractor and not someone else.

Third-Party Access Governance[1]

Managing non-employee onboarding without a centralized process is a challenge that leads to a variety of different workflows. Setting up accounts and granting permissions are inconsistent across the board. Without a direct means of flagging accounts as temporary or mapping them back to their respective sponsors, orphaned accounts can persist well beyond their acceptable lifespan, creating challenges for maintaining compliance.

Additionally, visibility into the full scope of the onboarded vendor’s access must be maintained in the system to ensure compliance.

If these third parties are left unchecked, the decentralized system cannot assure appropriate usage of access or follow-up, and the user’s access is still active. To combat these risks, organizations must have a consistent methodology for onboarding vendors, ensuring full visibility into an identities access, and managing the lifecycle of their access from onboarding to decommissioning.

Many modern organizations require the use of contractors or vendors, known as third parties. Managing these non-employees through the HR system, the authoritative identity source for their IT ecosystem is burdensome. In addition, third-party individuals often require access to organizational resources such as shared tools, applications, or data sets to provide critical services, but that access is often for a limited period.

Third parties present challenges and bring additional risks, such as ensuring that access is managed correctly and, when required, deprovisioned quickly. Saviynt plays a key role in helping many organizations simplify the vendor access management process and reduce non-employee risks. A robust vendor access management from the Saviynt Platform helps reduce these risks utilizing a sponsor-based approach to vendor access. Automation, access request, risk visibility, and access review are provided by Saviynt throughout the process of onboarding third parties and managing these identities throughout their lifecycle.

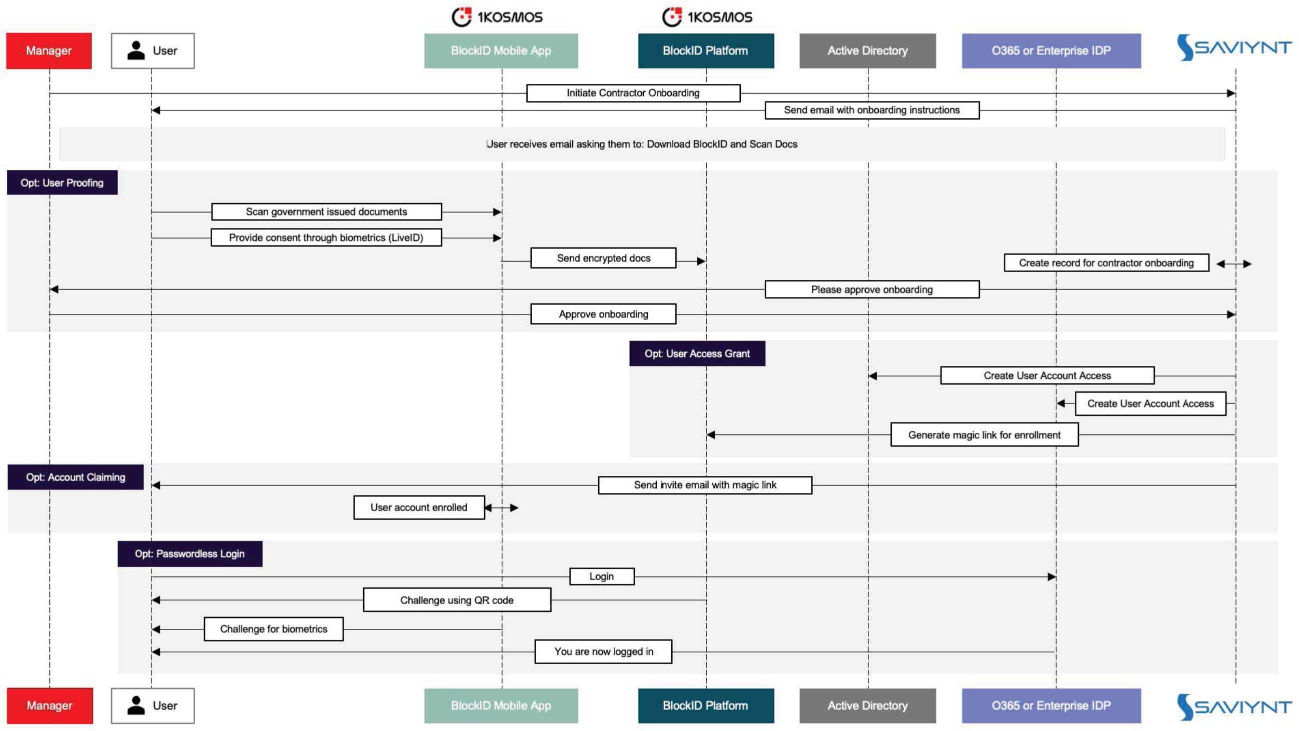
[1] From Saviynt TPAG Onboarding

The integration of Third-Party Access Governance and Identity Based Authentication

A new worker has to be verified before they are granted access to the infrastructure, and that access comes with a host of entitlements. But the gap remains: who verifies and who onboards the identity? As we've discussed, the need for combining strong identity assurance with strong third-party access governance is a logical approach to managing this common but poorly addressed issue.

How it works

Saviynt TPAG is integrated with 1Kosmos through the Universal Web Login interface that aids in the proofing and secure collection of PII data necessary for a contractor's automated onboarding. The UWL interface automates the API calls that need to be made from Saviynt into the 1Kosmos platform and the mobile app where the user would proof themselves. Through the partnership between 1Kosmos and Saviynt, the utility extends into account claiming through magic links that enable day zero onboarding of contractors through a high degree of assurance per NIST 800-63-3 standards.



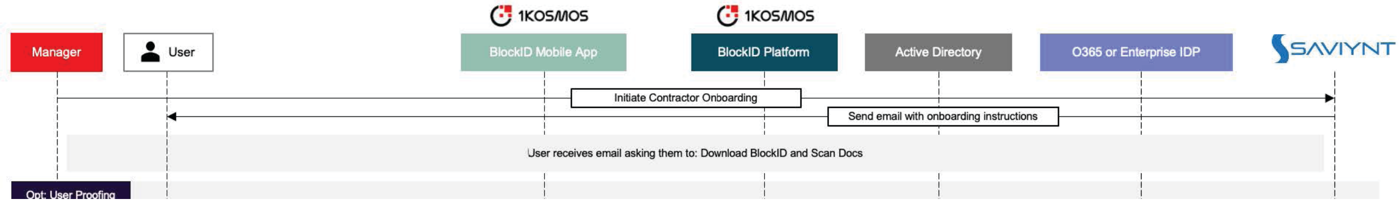
Saviynt, through its plethora of target connectors, can provision accounts and access into both on-premise and cloud systems seamlessly. The applications themselves are integrated either with 1Kosmos directly or with an IDP, thereby enabling a newly onboarded user to login into critical applications without Contractor Enrollment and Onboarding ever needing a password while preserving security through true biometric authentication from a registered device.

1Kosmos is built with specific capabilities for the onboarding, verification, and authentication of employees and contractors within the confines of the workplace. In this instance, 1Kosmos will validate the contractor onboarding and enrollment into the organization, leveraging Saviynt Third-Party Access Governance as their identity provider. The reference diagram illustrates how the two solutions work together but let's dig deeper into it.

Contractor Verification

1. The manager initiates the new hire. A new contractor is entered, and onboarding is initiated through Saviynt Third-Party Access Governance.

2. Saviynt Third-Party Access Governance generates and sends an email to the new contractor with onboarding instructions. <Saviynt generates a link in the email containing an embedded identifier for the user.>


1KOSMOS
1KOSMOS
Manager
User
BlockID Mobile App
BlockID Platform
Active Directory
O365 or Enterprise IDP
SAVIYNT
Initiate Contractor Onboarding
Send email with onboarding instructions
User receives email asking them to: Download BlockID and Scan Docs
Opt: User Proofing

User Proofing

1. The contractor downloads 1Kosmos app or a custom app integrated with 1Kosmos API from AppStore or Google Play.

2. The 1Kosmos Platform instructs the contractor to scan government-issued documents to proof themselves to and verify their identity to IAL2.

3. The contractor clicks the link in the email to start the onboarding process. The link displays a QR code generated by 1Kosmos for the contractor to begin sharing their proofed identity.

4. The new contractor is asked to provide consent through biometrics (1Kosmos Live ID) for sharing their PII data with Saviynt Third-Party Access Governance.

5. The captured documents are encrypted by the 1Kosmos Platform and are sent to Saviynt Third-Party Access Governance.

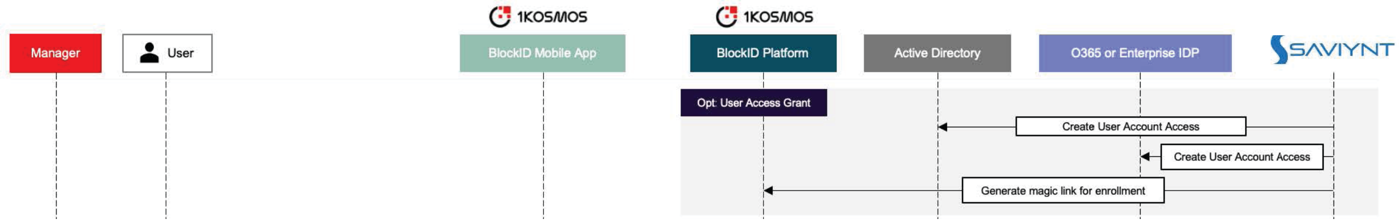
6. Saviynt Third-Party Access Governance decrypts documents and creates a record for the hiring manager to approve onboarding.

7. Saviynt Third-Party Access Governance sends an email to the hiring manager to log in, view, and approve onboarding.

User Access Grant

1. Saviynt Third-Party Access Governance creates an account and access in Microsoft Active Directory for O365 or an Enterprise IDP.

2. Saviynt Third-Party Access Governance sends a request to 1Kosmos Platform to generate a magic link for the contractor enrollment and account claiming.

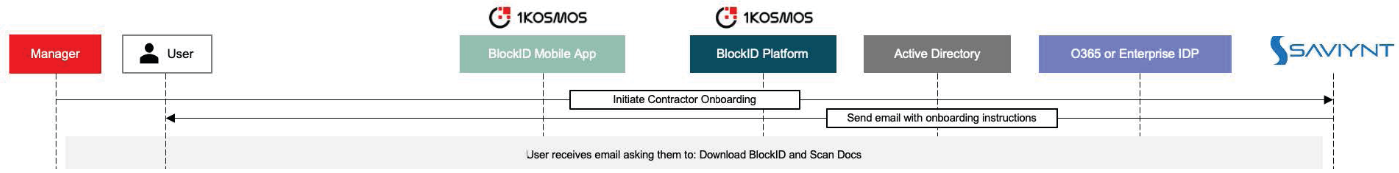


Account Claiming

1. Saviynt Third-Party Access Governance sends the new contractor an account claiming invite email with a magic link generated by the 1Kosmos platform.

2. The new contractor clicks the magic link and is challenged to provide MFA in the 1Kosmos mobile app through an OTP by email or SMS.

3. The contractor enterprise account is enrolled and bound to the contractor's mobile device within the mobile app.


1KOSMOS
1KOSMOS
Manager
User
BlockID Mobile App
BlockID Platform
Active Directory
O365 or Enterprise IDP
SAVIYNT
Initiate Contractor Onboarding
Send email with onboarding instructions
User receives email asking them to: Download BlockID and Scan Docs

Passwordless Login

1. The contractor, on their first day, will log in to O365.

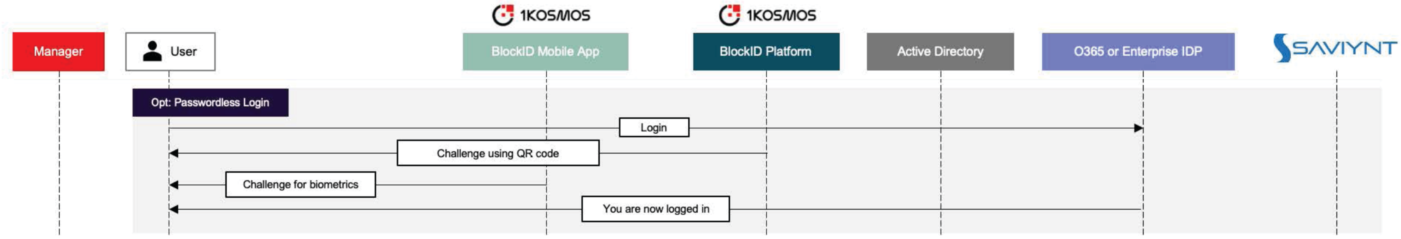
2. Office O365 or Enterprise IDP will trigger access with a SAML redirect to the 1Kosmos Platform.

3. The contractor will be challenged with a QR code. The contractor will scan the QR code with the 1Kosmos mobile app or custom app and is asked to provide their biometrics for access.

4. The contractor provides their Live ID.

5. The 1Kosmos Platform sends the authentication information to O365 or Enterprise IDP via a SAML response.The contractor is now logged in.

6. The contractor is now logged in.



The Business Outcomes

Saviynt defines third-party access governance as managing nonemployees, managing the identities and access entitlements of a partner, affiliate, volunteer, contractor, or vendor. Ultimately, most organizations have many contractors within their environments and have access to the infrastructure, applications, and data. The Saviynt Third Party Access Governance solution manages the life cycle, the onboarding, the entitlements, the governance of these third-party identities and, their authentication. 1Kosmos improves these capabilities by delivering a distributed digital identity platform that is both FIDO2 and NIST certified.

1Kosmos transforms the Saviynt Third Party Access Governance onboarding process. The result is the highest degree of identity assurance for new contractors. By binding contractors to their proofed identity, 1Kosmos creates an identity-based biometric authentication and a passwordless experience. Contractors will utilize their trusted mobile device for physical or logical daily authentication and step-up authentication required for privileged activities. As a result, each access event is associated with a real, verified identity.

When 1Kosmos is integrated with Saviynt Third Party Access Governance, you quickly move toward a Zero-Trust model, where 'never trust, always verify' results from the combined solutions. 1Kosmos provides the proof of who somebody is, verifying users using biometrics, and will eliminate the contractor jacking highlighted above. In addition, Saviynt Third Party Access Governance manages the identity life cycle, entitlements, and the governance of these third-party identities.

Combining the technologies from1Kosmos and Saviynt addresses the challenges organizations face dealing with contractors. Organizations will manage the identity governance of contractors, securely enroll and onboard the contractor to a passwordless environment, eliminating user names and passwords and eliminating contractor jacking potential. Overall, organizations will eliminate the extra security exposures contractors introduce.

About 1Kosmos

1Kosmos enables remote identity verification and passwordless multi-factor authentication for workers, customers and residents to securely transact with digital services. By unifying identity proofing, credential verification and strong authentication, the 1Kosmos platform prevents identity impersonation, account takeover and fraud while delivering frictionless user experiences and preserving the privacy of users' personal information. 1Kosmos performs millions of authentications daily for government agencies and some of the largest banks, telecommunications, higher education, and healthcare organizations in the world.