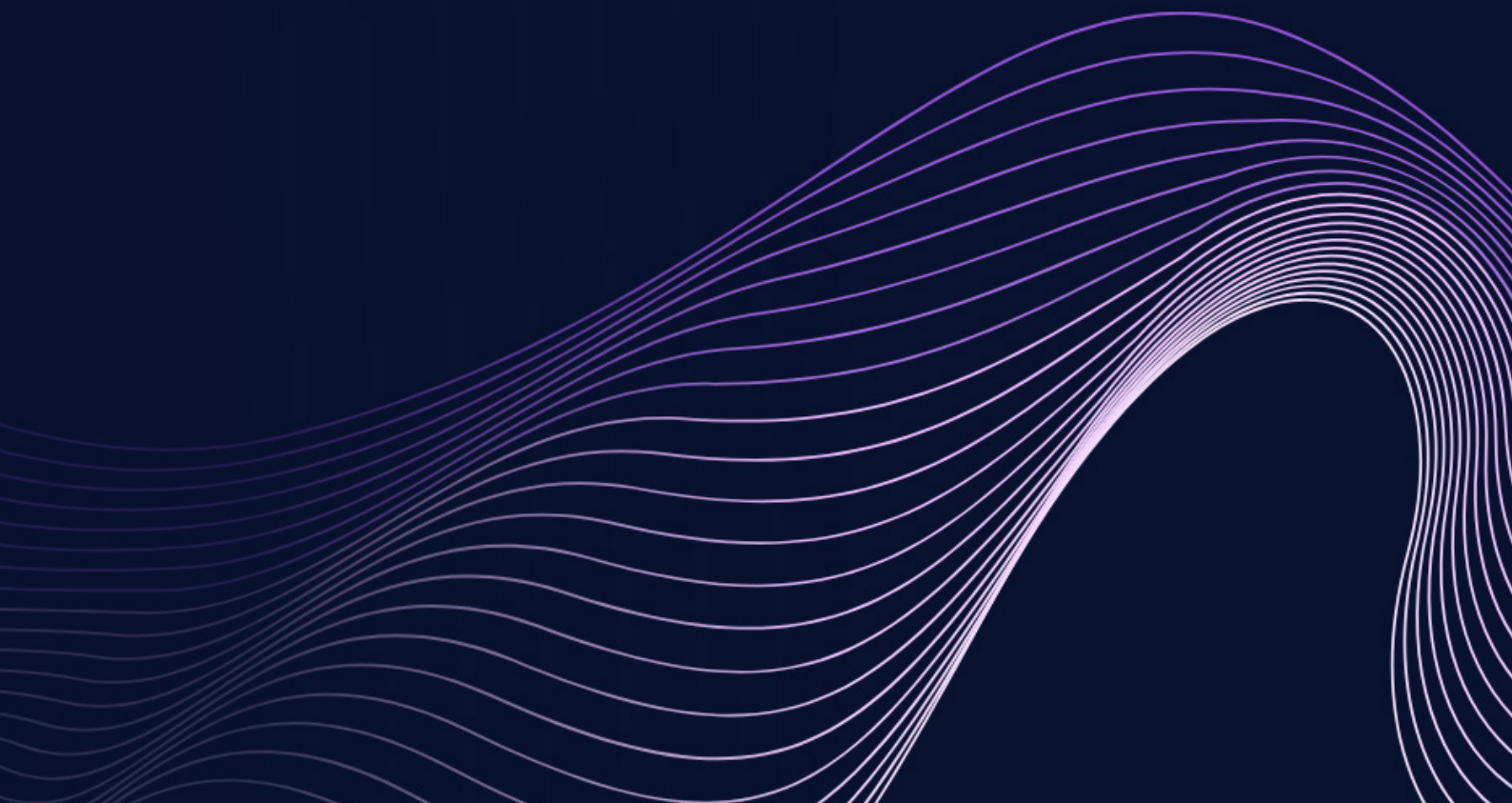




Brochure

Secure and efficient
management solution for
external digital identities



The situation

The workforce of an average organisation consists for 20% out of external / third party identities.



Several severe challenges arise because the HRM system and HR processes are not designed with third-party identity life cycle management in mind. This has a serious impact on efficiency, security and cost.

The challenge

- ⊘ Accounts for third-party identities not revoked due to lack of 'end of contract trigger' in HR process
- ⊘ Access rights for third-party contractors not available on start date
- ⊘ Processing and storage of data of third-party contractors leads to GDPR violations.
- ⊘ Low quality input for IAM process resulting from data errors due to manual data entry in the HR system
- ⊘ Third-party contractor data leads to pollution of the HR systems statistics and reports
- ⊘ High costs and redundant workload for managing third-party contractors in expensive HRM system

The solution = iD Veritas

The iD-Veritas solution is purpose-built for third-party identity life cycle management. It feeds the third-party identity data into your IGA solution of choice, using open standards and/or APIs.



Features and solution overview

- ✓ Cloud based portal for third-party self-service identity lifecycle management
- ✓ Data management via webform, csv upload aor API connection
- ✓ Third-party identity data delivered real time to IAM tooling
- ✓ IAM userID for third-party employees used throughout the data chain
- ✓ Attestation and approval for release of third-party identity data to IAM tooling by third-party manager or by the responsible manager within your organization
- ✓ Authentication by federation or ID-Veritas IDP



Achieve control in 5 steps

All external identities in iD Veritas >

Be in firm control of the lifecycle of identities (J/M/L) >

Connect to your IAM solution >

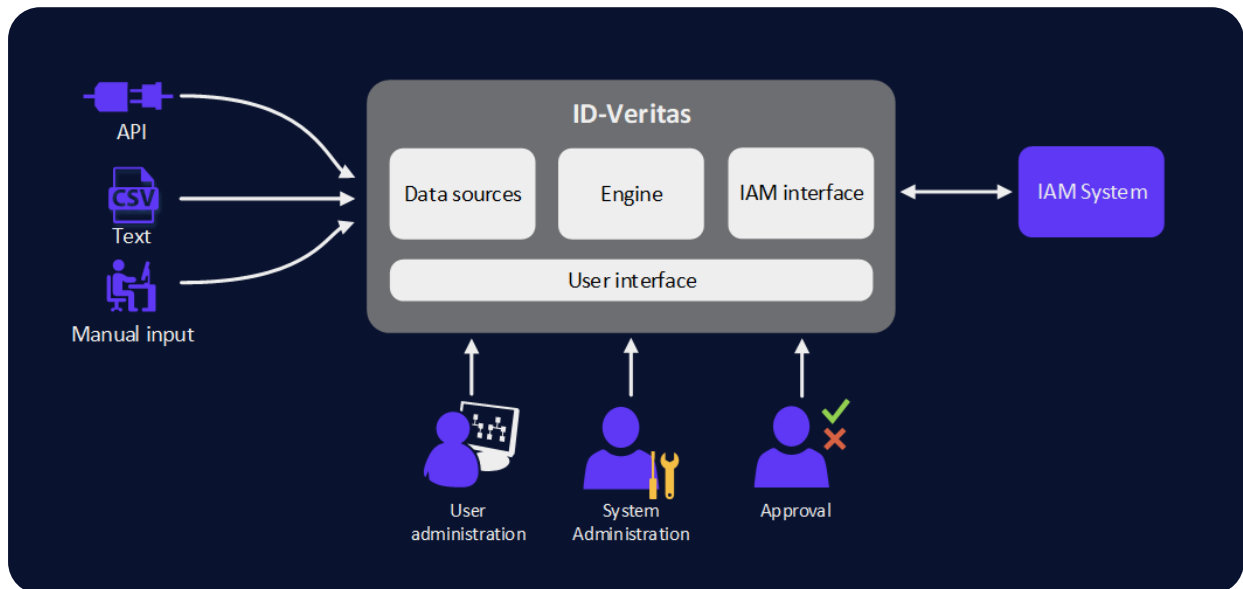
Outsource identity data management to your resourcing partners >

Maintain control and insight through recertification >

Verified identity data as input for the IAM-process results in high-quality output

Solution Design

Security Architecture



- ✓ Strong authentication against ID-Veritas IDP or by federation.
- ✓ Hard separation of Customer and Third-Party data.
- ✓ Least privilege role model.
- ✓ Cryptographic key management (PKBDF2).
- ✓ Microsoft malware- and virus security.
- ✓ Network security best practices.
- ✓ Microsoft Azure network security groups.
- ✓ HTTPS / TLS/SSL encryption.



Benefits of iD Veritas

- ✔ Efficient on- and off-boarding process for third-party identities.
- ✔ In control of the third-party identities life cycle (J/M/L).
- ✔ Compliant with data-storage regulations.
- ✔ High quality input for the IAM solution resulting in high quality IAM output.
- ✔ Eliminate use of expensive HRM licenses for third-party identities.

[Book a demo](#)



Contact

If you'd like to know more about the possibilities of managing external identities with iD Veritas, then contact us on +31 (0)88 - 998 2020, sales@id-veritas.com or visit www.id-veritas.com.

We look forward to hearing from you!

