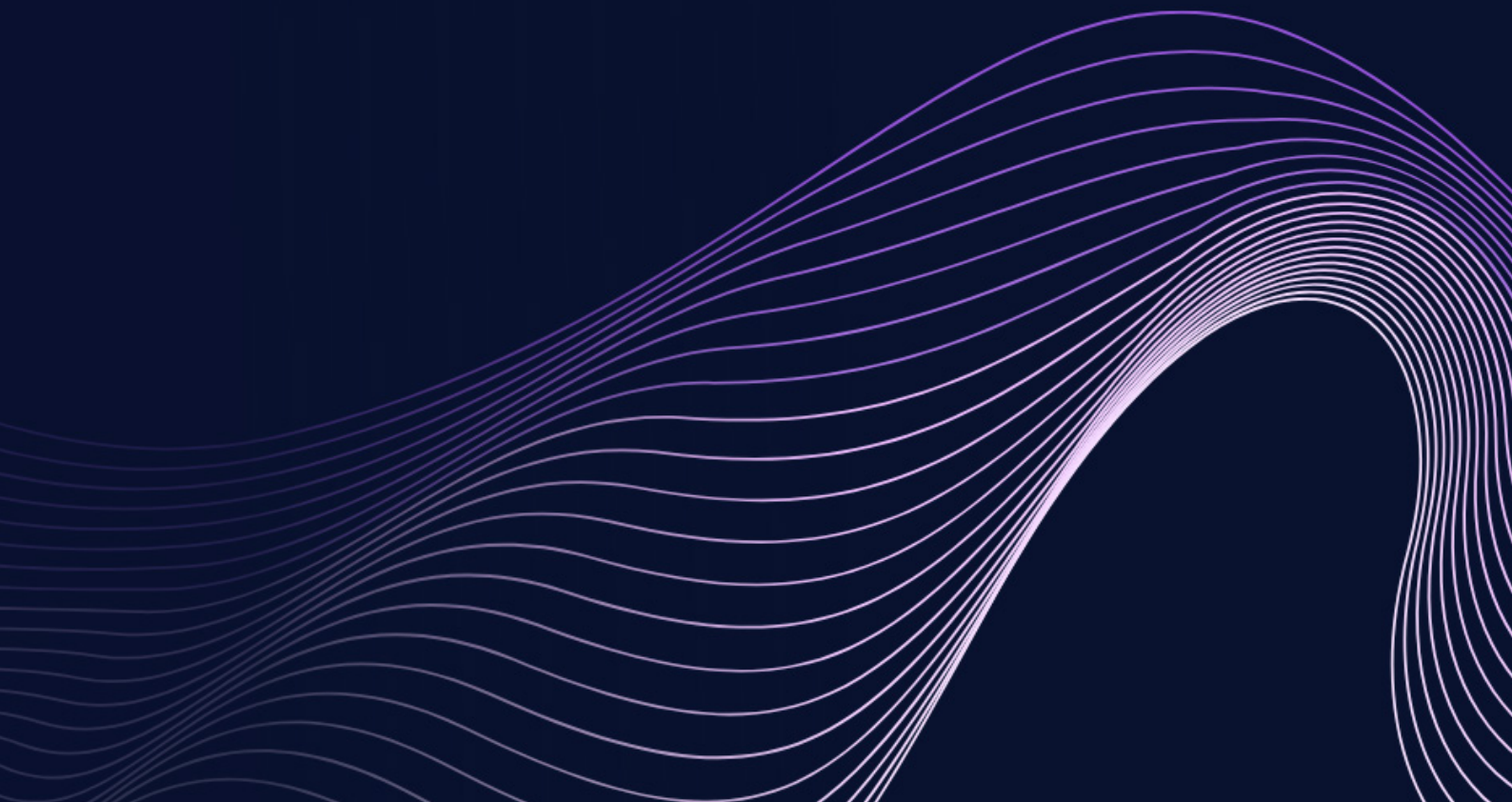
Veritas

Whitepaper

Veilig beheer van identiteitsdata van externe identiteiten in de financiële sector



Introductie

De omarming van het hybride werken en de verschuiving naar online dienstverlening heeft veel kansen gecreëerd voor de financiële sector. Zo kunnen diensten beter en op ad hoc basis worden op- en afgeschaald, waardoor de sector nu flexibeler is dan ooit tevoren. Daarmee is de behoefte aan externe medewerkers de afgelopen jaren exponentieel gegroeid en deze verschuiving brengt ook uitdagingen met zich mee. Met name op het gebied van IT. Veel processen waarbij externe medewerkers betrokken zijn worden nog steeds handmatig uitgevoerd, waardoor ze foutgevoelig, tijdrovend en daarmee ook kostbaar zijn.

In deze whitepaper leest u hoe de identiteitsgegevens van externe medewerkers, ofwel externe identiteiten, het best kunnen worden beheerd en hoe u dat op een veilige en efficiënte manier kunt doen.

De uitdaging van het beheren van externe identiteiten

De processen voor het onboarden van interne medewerkers zijn vaak goed vastgelegd en hun identiteitsdata wordt meestal opgeslagen in het HR-systeem. Als het echter om externe identiteiten gaat, zijn er veel uitdagingen. Volgens de wet- en regelgeving mogen niet alle gegevens van externe identiteiten worden opgeslagen in het HR-systeem van uw organisatie, maar vanwege efficiency wordt dit vaak wel gedaan. Financiële instellingen worstelen dan ook met de manier om externe identiteiten veilig en efficiënt op te slaan.

Gelukkig kan de introductie van nieuwe technologieën helpen de gegevens van externe identiteiten op een veilige manier te beheren. Deze nieuwe technologieën kunnen ervoor zorgen dat alle noodzakelijke gegevens op een conforme manier worden vastgelegd.

Voor interne medewerkers worden rollen en rechten vaak via een IAM-oplossing (Identity & Access Management) toegekend, terwijl voor externe medewerkers veelal andere en handmatige processen worden ingezet. Door gebruik te maken van nieuwe technologieën kunt u de toepasselijke wet- en regelgeving naleven, terwijl u ook de essentiële informatie krijgt die nodig is om externe werknemers te onboarden.

Controle over data van externe identiteiten

Om identiteitsgegevens van externe identiteiten veilig te beheren en ervoor te zorgen dat externe medewerkers de juiste toegang hebben wanneer dat nodig is, is het belangrijk de controle over de identiteitsdata te nemen en te houden. De lifecycle (joiners/movers/leavers) van externe identiteiten is namelijk anders dan die van interne medewerkers.

Voor het onboardingproces van nieuwe externe medewerkers (joiners) is het essentieel om hen op het juiste moment toegang te geven, zodat ze direct aan de slag kunnen. Ook wanneer externe medewerkers van functie veranderen of ander werk toegewezen krijgen (movers), moet u ervoor zorgen dat zij de nodige toegang krijgen en dat onnodige toegang wordt ingetrokken. Zo kunt u de identiteitsgegevens van externe identiteiten veilig beheren en ervoor zorgen dat externe medewerkers te allen tijde de juiste toegang hebben.

De offboarding wordt niet altijd secuur uitgevoerd, vaak is het niet overal duidelijk wanneer een externe medewerker stopt met het uitvoeren van zijn werkzaamheden en er dus geen standaard proces kan worden uitgevoerd waarmee de toegang en rechten van de betreffende externe identiteit worden ingetrokken. Als toegang aan het einde van de werkperiode niet wordt ingetrokken, loopt u het risico dat de accounts en toegangsrechten van de externe identiteiten (leavers) onnodig of ongewenst open blijven staan en dit levert onnodige veiligheidsrisico's op.

Met iD Veritas kunt u de gehele lifecycle van externe identiteiten beheren. Wanneer bijvoorbeeld de einddatum van een contract is bereikt, stuurt iD Veritas automatisch een seintje naar uw IAM-oplossing, zodat de IAM-oplossing de bijbehorende toegang en rechten kan intrekken. Zo hebben externe identiteiten nooit langer toegang dan nodig en voorkomt u onnodige security risico's.

Veilig beheer van identiteitsdata

Door risico's te minimaliseren en duidelijk toezicht te houden op wie toegang heeft tot wat, draagt uw IAM-oplossing bij aan betere informatiebeveiliging. Om uitdagingen op het gebied van extern identiteitsbeheer aan te pakken, hebben organisaties een oplossing nodig:

- die ervoor zorgt dat volledige en zuivere data automatisch in uw IAM-oplossing terecht komt;
- die naadloos integreert met de IAM-oplossing en die aantoonbare controle biedt over de toegang, rollen en machtigingen van externe identiteiten in de IT-omgeving van uw organisatie;
- die bijdraagt aan het minimaliseren van risico's;
- en die aantoonbaar controle geeft over de toegang, rollen en rechten van externe identiteiten in de IT-omgeving van uw organisatie.

Hoe helpt iD Veritas?

Met iD Veritas gekoppeld aan uw IAM-oplossing kunt u efficiënter werken en de kans op fouten verkleinen waardoor het toegangsbeheer voor externe identiteiten veilig, doeltreffend en efficiënt is geregeld.

Bovendien bent u in staat om het on- en offboarding proces voor externe identiteiten op een veilige, efficiënte en gecontroleerde wijze uit te voeren. Daarbij bent u volledig in controle over de gehele lifecycle. Dit doet u in 5 stappen:

1 Alle externe identiteiten in iD Veritas

Breng alle externe identiteiten naar iD Veritas door ze handmatig in te voeren, upload een CSV-overzicht of sluit iD Veritas aan op de database van uw leverancier (via een API). Dit zorgt voor één centrale bron van zuivere data van de externe identiteiten in uw organisatie.

2 De lifecycle van externe identiteiten

Externe identiteiten komen uw organisatie binnen, ze veranderen misschien tussentijds van rol/functie en na verloop van tijd komt hun contract tot een einde. In iD Veritas kunt u de volledige lifecycle (ook bekend als het Joiner-Mover-Leaver process) van uw externe identiteiten beheren en geautomatiseerd laten uitvoeren.

3 Aansluiting op uw IAM-oplossing

iD Veritas is aan te sluiten op elke Identity and Access Management-oplossing op de markt. Via open standaarden (zoals een API) verstuurt en ontvangt iD Veritas informatie van en naar uw IAM-oplossing. Uw IAM-partner kan deze aansluiting tussen iD Veritas en uw IAM-oplossing voor u verzorgen. Geen IAM-partner? Dan staan The Identity Managers voor u klaar.

4 Besteed het werk uit aan uw resourcing partners

U heeft de keuze om het beheer van data van de externe identiteiten aan uw resourcing partners uit te besteden. Zo besteedt u de administratieve werkzaamheden zoals het opvoeren, aanpassen en verwijderen van de externe identiteiten uit. Uw organisatie hoeft dan alleen de ingevoegde informatie te valideren. Makkelijk en efficiënt!

5 Behoud controle en inzicht

Dankzij de security-by-design architectuur en privacy-by-default functionaliteit voor een absolute scheiding van data beheert u veilig de identiteitsdata van uw externe identiteiten. Met standaard functionaliteiten zoals een her-certificeringsproces en uitgebreide rapportage mogelijkheden bent u niet alleen in controle, maar kunt u dit ook aantonen. Daarmee wordt het voldoen aan wet- en regelgeving een stuk eenvoudiger.

iD Veritas

Contact

Geïnteresseerd in de mogelijkheden voor het beheren van externe identiteiten met iD Veritas? Neem dan contact met ons op via 088-9982020, sales@id-veritas.com of bezoek www.id-veritas.com. Wij horen graag van u!