Standaard Logische Toegangsbeveiliging

Beleidsregels voor de beveiliging van digitale toegang tot producten, diensten, gegevens en bedrijfsmiddelen van het Kadaster

Versie

4.0

Auteur(s)

LTB

Standaard Logische Toegangsbeveiliging

Beleidsregels voor de beveiliging van digitale toegang tot producten, diensten, gegevens en bedrijfsmiddelen van het Kadaster

Opdrachtgever
CISO

Status
Definitief

Verspreiding
Bedrijfsvertrouwelijk

Versiehistorie

Versie	Datum	Auteur	Opmerking
2.0	23 mei 2018	LTB	Goedgekeurd door DR
3.0	Mei 2021	LTB	Versie voor goedkeuring Risk Committee
4.0	Maart 2025	LTB	Update na review

Recensiehistorie

Versie	Datum	Recensent	Opmerking
2.0	23 mei 2018	DR	Opmerkingen DR verwerkt
3.9	februari 2025	Sam Besselink, Nico Nimeijer, Patrique Burgersdijk, Merel Bakker, Rob Messelink, Dietmar Timmerman, Niels Sombekke	

Inhoudsopgave

1 Standaard Logische Toegangsbeveiliging

1.1 Inleiding

Toegangsbeveiliging omvat twee hoofdgebieden: fysieke en logische toegangsbeveiliging. Fysieke toegangsbeveiliging richt zich op de toegang tot gebouwen, papieren dossiers en apparatuur. Logische toegangsbeveiliging richt zich op de toegang tot producten, diensten, gegevens en bedrijfsmiddelen, zoals applicaties, systemen en databases.

Dit document beschrijft de beleidsregels voor logische toegangsbeveiliging binnen het Kadaster.

1.2 Noodzaak

Deze standaard biedt kaders om ongeautoriseerde toegang tot alle producten, diensten, gegevens en bedrijfsmiddelen van het Kadaster te voorkomen. Dit omvat bijvoorbeeld alle applicaties, systemen en databases. De maatregelen zijn bedoeld om ongeautoriseerde handelingen en acties tegen te gaan en zo de integriteit, vertrouwelijkheid en beschikbaarheid van informatie te waarborgen.

1.3 Doelstelling(en)

Het Kadaster hanteert de volgende doelstelling voor logische toegangsbeveiliging:
Het waarborgen van gecontroleerde toegang voor subjecten, zoals medewerkers, leveranciers, gasten, kandidaten, applicaties en systemen tot objecten (applicaties, systemen en databases), zoals producten, diensten, gegevens en bedrijfsmiddelen op basis van passende identificatie, authenticatie, autorisatie en logging en monitoring. Dit om de risico's op schade door onbevoegd gebruik te beheersen.

Dit document beschrijft de geldende beleidsregels op het gebied van logische toegangsbeveiliging, zodat de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens van het Kadaster en informatie in producten, diensten en bedrijfsmiddelen van het Kadaster juist, volledig en controleerbaar beschermd worden. Het beleid is gebaseerd op de ISO27001 standaard en de Baseline Informatiebeveiliging Overheid (BIO).

1.4 Reikwijdte

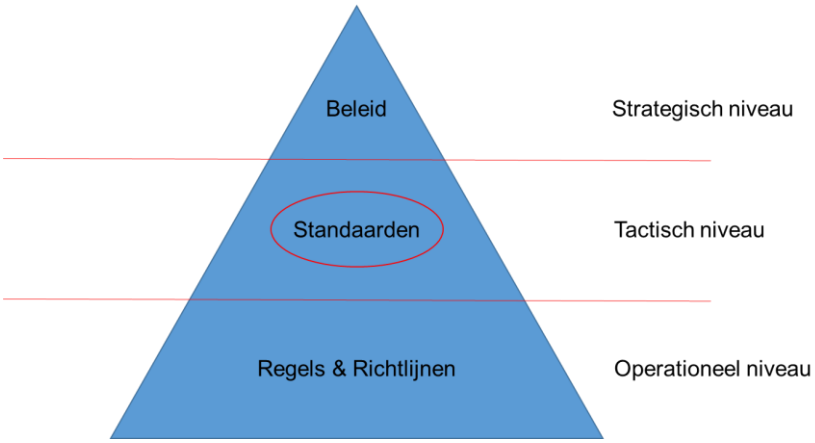
Dit beleid is van toepassing op het gehele Kadaster en geldt voor alle medewerkers en gelijkgestelden, zoals extern ingehuurde medewerkers, flexwerkers en derden die diensten leveren aan het Kadaster. De beleidsregels zijn ook van toepassing bij de uitbesteding van diensten.

1.5 Eigenaarschap

De eigenaar van deze standaard is de directeur van de directie Data, Governance en Vernieuwing. De actiehouders van deze standaard zijn de verschillende diensteigenaren binnen het kadaster. Diensteigenaren zijn verantwoordelijk voor de naleving van dit beleid binnen hun werkgebied.
Herijking gebeurt periodiek volgens de richtlijnen van het Kadaster Informatiebeveiligingsbeleid. De CISO bewaakt het proces en initieert herijkingen indien nodig.

1.6 Positionering

Deze standaard valt onder het Kadaster Informatiebeveiligingsbeleid. Deze standaard beschrijft zowel de tactische beleidsregels als de uitwerkingen op operationeel niveau, waar operationele regels en richtlijnen naar kunnen verwijzen.



Figuur 1 Positie van dit document in het Informatiebeveiligingsbeleid

1.7 Pas-toe-of-leg-uit

Deze standaard past het bovenliggende Informatiebeveiligingsbeleid toe. Afwijkingen zijn alleen toegestaan mits de procedure voor uitzondering op beleid wordt gevolgd.

1.8 Definities

De gehanteerde definities zijn opgenomen in de bijlage.

1.9 Randvoorwaarden

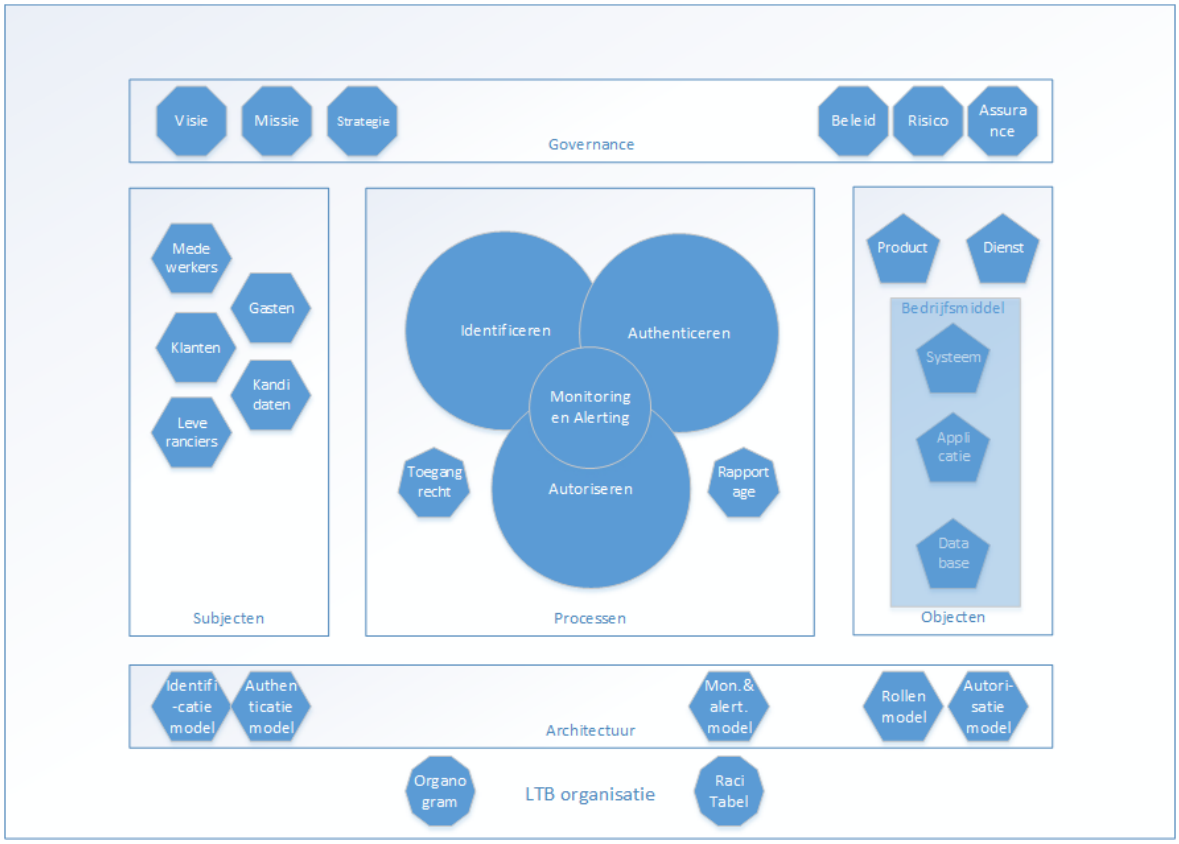
- Actuele en volledige identiteitsgegevens van vaste en extern ingehuurde medewerkers uit HR-systemen, en identiteitsgegevens van leveranciersmedewerkers uit het contractmanagementsysteem, zijn vereist voor effectieve toegangsbeveiliging.
- Een gedetailleerde en actuele Configuration Management Database (CMDB) die alle diensten, applicaties en systemen documenteert, vormt de basis voor het beheer van toegangsrechten en wijzigingen in de IT-omgeving.
- Een effectief risicomanagementsysteem met een duidelijke rolverdeling tussen de tweede lijn (risicomanagement en compliance) en de derde lijn (interne audit) draagt bij aan de implementatie, handhaving en periodieke evaluatie van het toegangsbeveiligingsbeleid.
- Een centraal monitoring- en logging-systeem voor het detecteren en analyseren van afwijkend gedrag, met duidelijke verantwoordelijkheden voor het opvolgen van beveiligingswaarschuwingen.

2 Standaard Logische Toegangsbeveiliging

2.1 Model Logische Toegangsbeveiliging

De beleidsregels zijn gebaseerd op het model zoals weergegeven in figuur 2, dat verschillende elementen binnen logische toegangsbeveiliging schetst, zoals governance, identificeren authentiseren en autoriseren. Dit model wordt verder uitgewerkt in de solution architectuur voor logische toegangsbeveiliging. De essentie is het waarborgen van gecontroleerde toegang van subjecten (zoals medewerkers en systemen) tot objecten (zoals producten en diensten).

De begrippen die in dit model en beleid worden gebruikt, zijn nader toegelicht in de begrippenlijst in de bijlage. In de volgende hoofdstukken worden de beleidsregels per element van dit model beschreven, zoals governance & organisatie, identificeren, authentiseren en autoriseren.



Figuur 2 Model Logische Toegangsbeveiliging

3 Organisatie & Governance

3.1 Eigenaarschap producten, diensten, gegevens en bedrijfsmiddelen

Alle diensten waartoe rechten worden toegekend hebben een eigenaar. Deze eigenaar is verantwoordelijk voor de beveiliging, en daarmee ook voor de logische toegangsbeveiliging van de dienst. De lijnmanager is verantwoordelijk voor de toegangsrechten van vaste en extern ingehuurde medewerkers (zie paragraaf 3.3). De diensteigenaar (applicatie- of data eigenaar) bepaalt wie, onder welke condities toegang krijg tot de dienst binnen de kaders van het LTB-beleid. Deze rechten worden vastgelegd in het Autorisatieportaal (zie paragraaf 3.2).

3.2 Verantwoordelijkheid diensteigenaar

De diensteigenaar is verantwoordelijk voor het registreren en beheren van toegangsrechten, in samenwerking met de data-eigenaar. Toegangsrechten, inclusief voorwaarden waaronder deze worden uitgegeven (zoals afdelings- en/of functiebeperkingen, aanvullende goedkeurders en risicoclassificatie), worden vastgelegd en goedgekeurd in het Autorisatieportaal door de diensteigenaar of, waar relevant, de data-eigenaar. De diensteigenaar is vastgelegd in de CMDB. Binnen één applicatie kunnen meerdere data-eigenaren bestaan, waarbij elke dataset een specifieke data-eigenaar kan hebben. De data-eigenaar is in alle gevallen eindverantwoordelijk voor de toegangsrechten tot de data. Het is van belang dat de diensteigenaar ook wijzigingen in toegangsrechten registreert als wijzigingen in de dienst hier aanleiding toe geven (via change management).
Er zijn processen ingericht om ervoor te zorgen dat de verantwoordelijke dienst- en data-eigenaren actueel blijven in het LTB-systeem bij instroom, doorstroom en uitstroom.

3.2.1 Periodieke controle van de dienst en de toegangsrechten

Om toegangsrechten juist en volledig te houden, beoordeelt de diensteigenaar (of waar relevant: de data-eigenaar) minimaal jaarlijks:

- of het eigenaarschap en de vastgelegde dienst- en data-eigenaren nog correct zijn;
- of de voorwaarden waaronder toegangsrechten mogen worden uitgegeven (zoals afdelings- en/of functiebeperking of aanvullende goedkeurders) nog actueel en passend zijn.

De resultaten van deze controles worden gedocumenteerd en besproken met relevante betrokkenen om noodzakelijke acties te ondernemen.

3.3 Verantwoordelijkheid lijnmanager

De lijnmanager is verantwoordelijk voor de toegangsrechten van vaste en extern ingehuurde medewerkers. Deze rechten mogen alleen worden toegekend binnen de kaders gesteld door de diensteigenaar (zie ook paragraaf 5.2). De lijnmanager weet welke werkzaamheden medewerkers uitvoeren en draagt de operationele verantwoordelijkheid voor deze medewerkers.
De lijnmanager is verantwoordelijk voor:

- het toepassen van het ‘least privilege’ principe bij het toekennen van toegangsrechten aan medewerkers;
- het toekennen en intrekken van toegangsrechten bij instroom, doorstroom en uitstroom van medewerkers;
- het minimaal jaarlijks beoordelen van de toegekende toegangsrechten de eigen medewerkers.

Er zijn processen ingericht om ervoor te zorgen dat de verantwoordelijke lijnmanagers actueel blijven in het LTB-systeem bij instroom, doorstroom en uitstroom.

4 Identiteiten- en accountbeheer

4.1 Identiteiten en accounts

Autorisatiebeheerprocessen (IGA-processen) zorgen ervoor dat de identiteiten van medewerkers in de centrale administratie en hun toegangsrechten worden vertaald naar accounts in applicaties met de bijbehorende permissies. Deze autorisatiebeheerprocessen waarborgen dat alle accounts en hun eigenaren geregistreerd en actueel zijn.

Accounts zijn essentieel om verschillende gebruikers in applicaties en systemen van elkaar te onderscheiden. Elk account heeft een eigenaar die verantwoordelijk is voor het gebruik van het account. Een persoon kan meerdere accounts hebben voor toegang tot verschillende applicaties. Daarnaast bestaan er onpersoonlijke accounts, die niet zijn gekoppeld aan een specifieke gebruiker, maar een ander doel dienen (ook bekend als niet-persoonsgebonden accounts, NPA's).

4.2 Registratie van identiteiten

Alle identiteiten van personen worden geregistreerd, inclusief eventuele aanstellingen en/of detacheringen van de persoon bij het Kadaster:

- het identificeren van vaste en extern ingehuurde medewerkers is onderdeel van het in-dienst proces;
- het identificeren van leveranciers is onderdeel van het contractmanagementproces;
- het identificeren van bezoekers valt onder de standaard fysieke toegangsbeveiliging.

Voor andere samenwerkingen dan met externe medewerkers leveranciers, kan logische toegang nodig zijn. Hiervoor kunnen gasten worden uitgenodigd, bijvoorbeeld voor deelname aan een Teamssite. Voor het faciliteren van logische toegang voor dergelijke partijen middels 'gasten' is er een verkorte toetsing om samenwerking te beoordelen. Per partij is toestemming nodig van de security officer. Externe partijen zijn zelf verantwoordelijk voor de identificatie van hun eigen medewerkers en ingehuurde krachten.

4.3 Specifieke accounts voor kritieke toegang

Accounts met kritieke toegang kunnen aanzienlijke schade veroorzaken en zijn aantrekkelijke doelwitten voor kwaadwillenden. Het gebruik van kritieke toegang (ook wel uitzonderlijke toegang of (high) privileged toegang genoemd) vereist daarom specifieke accounts. De diensteigenaar is verantwoordelijk voor het classificeren welke toegang als 'kritiek' moet worden beschouwd, waarbij minimaal geldt:

- alle toegang is kritiek die beheeractiviteiten op productie omgevingen of omgevingen met productiedata mogelijk maakt;
- alle toegang is kritiek die het beïnvloeden van resources (bijvoorbeeld databases of virtuele servers) in productieomgevingen mogelijk maakt;
- alle toegang is kritiek die gebruik van systeemhulpmiddelen mogelijk maakt die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen[1];
- alle toegang is kritiek die beheer van permissies of aan gebruikers toegekende permissies mogelijk maakt;

[1] Voorbeelden hiervan kunnen zijn:
- beheertoegang op OS-niveau, inclusief gebruik van systeemhulpmiddelen via 'sudo',
- beheertoegang tot antivirus software, malware beschermingshulpmiddelen, update & patching mechanismen of back-up software,
- ontwikkelaarshulpmiddelen zoals debuggers of virtualisatieplatforms,
- netwerkbeheer en -monitoring hulpmiddelen.

- alle toegang is kritiek die beheer van gebruikersnamen, resetten van inloggegevens (waaronder MFA-middelen), of inzien van inloggegevens mogelijk maakt.

De maatregelen voor accounts met kritieke toegang staan in hoofdstuk 6 Authenticatie.

4.4 Ieder account heeft een eigenaar

Elk account heeft een eigenaar die verantwoordelijk is voor het gebruik van het account en het geheimhouden van de inloggegevens, zoals wachtwoord, private keys en tokens. Dit geldt uitdrukkelijk ook voor onpersoonlijke accounts.

4.5 Onpersoonlijke accounts

Onpersoonlijke accounts dienen een ander doel dan gebruik door een specifieke eigenaar. De eigenaar van het account is niet noodzakelijk de beoogde gebruiker, en het is mogelijk dat activiteiten met het account door meerdere gebruikers worden uitgevoerd. Voorbeelden van onpersoonlijke accounts zijn:

- serviceaccounts voor koppelingen tussen applicaties/systemen;
- default accounts die standaard zijn ingebouwd in applicaties/systemen;
- applicatie- en systeemaccounts die door beheerdersgroepen, voor tests of voor noodherstel worden gebruikt.

Het aanmaken, wijzigen, periodiek controleren en verwijderen van onpersoonlijke accounts is een centraal beheerd proces, tenzij ze zijn opgenomen in de centrale PAM-oplossing. Eigenaarschap en de reden voor het bestaan van onpersoonlijke accounts verdienen extra aandacht. Daarom moeten deze accounts centraal worden geregistreerd, tenzij ze in de centrale PAM-oplossing zijn ondergebracht.

Bij het aanvragen of aanmaken van een onpersoonlijk account is het essentieel om het minimum aan rechten toe te kennen (‘least privilege’) als onderdeel van ‘secure by design’. Dit komt omdat de permissies van onpersoonlijke accounts doorgaans minder vaak veranderen dan die van persoonlijke accounts.

Voor het eigenaarschap van onpersoonlijke accounts wordt onderscheid gemaakt tussen:

- onpersoonlijke accounts in centrale directories en vergelijkbare infrastructuur: deze moeten bij aanvang een toegewezen dienst als eigenaar hebben;
- onpersoonlijke accounts in applicaties en systemen: deze vallen onder de verantwoordelijkheid van de applicatie-eigenaar, tenzij een andere dienst is aangewezen als eigenaar.

Accounts zonder eigenaar mogen alleen in centrale directories voorkomen. Deze accounts moeten tijdig worden gedeactiveerd, waarbij belanghebbenden worden geïnformeerd. Nadat communicatie in relevante gremia heeft plaatsgevonden, moeten deze accounts binnen een maand worden gedeactiveerd. Het bestaan en beoogde gebruik van noodherstelaccounts (‘breaking glass accounts’) moeten worden gedocumenteerd in het herstelplan van de betreffende dienst. In de basis worden noodherstel accounts nooit gebruikt, tenzij zich er een crisisscenario voordoet.

4.5.1 Periodieke controle onpersoonlijke accounts

De noodzaak van onpersoonlijke accounts wordt jaarlijks beoordeeld door de eigenaren van de accounts. Afwijkingen en noodzakelijke correcties worden centraal geregistreerd.

4.5.2 Logging en monitoring

Beveiligingswaarschuwingen over onverwacht of afwijkend gebruik van onpersoonlijke accounts worden verstuurd naar relevante actoren. Deze waarschuwingen worden geregistreerd, gemonitord, geanalyseerd en opgevolgd via centrale security monitoring. Lessons learned worden toegepast om herhaling te voorkomen. Voor noodherstelaccounts geldt dat er altijd een register aanwezig moet zijn van gebruik van het account of dat vanuit de centrale security monitoring beveiligingswaarschuwingen verstuurd worden naar relevante actoren naar aanleiding van gebruik van het account. Ook deze beveiligingswaarschuwingen worden opgeslagen, geregistreerd, gemonitord, geanalyseerd en hersteld.

5 Autorisatiebeheer

5.1 Least privilege en functie- of rolscheiding

Om ongeautoriseerde toegang en beveiligings- en datalekken te voorkomen, wordt altijd het principe van ‘least privilege’ toegepast. Dit houdt in dat toegang beperkt blijft tot wat noodzakelijk is voor het uitvoeren van taken, bevoegdheden en verantwoordelijkheden. Wanneer verschillende soorten toegang conflicteren of de combinatie ervan een risico vormt, wordt functie- of rolscheiding verplicht toegepast om deze risico’s te minimaliseren.

5.2 Toegangsrechten toekennen, wijzigen en intrekken

Toegangsrechten worden uitsluitend via het LTB-systeem gewijzigd. Ze worden toegekend of ingetrokken na de benodigde goedkeuringen en in lijn met het principe van ‘least privilege’, waarbij toegangsrechten strikt beperkt blijven tot wat noodzakelijk is voor de uitvoering van taken, bevoegdheden en verantwoordelijkheden. Toegangsrechten worden ingetrokken wanneer ze niet langer nodig zijn, bijvoorbeeld bij functiewijzigingen, teamwisselingen of het ontbreken van goedkeuring tijdens periodieke controles. Bij doorstroom worden oude toegangsrechten ingetrokken en nieuwe rechten toegekend volgens de gestelde eisen en het principe van ‘least privilege’.

Lage, reguliere en kritieke rechten:

- Lage toegangsrechten behoeven in de basis geen goedkeuring van de lijnmanager.
- Reguliere toegangsrechten vereisen goedkeuring van de lijnmanager.
- Kritieke toegangsrechten vereisen goedkeuring van zowel de lijnmanager als de diensteigenaar van de betreffende dienst.

Goedkeuring van toegangsrechten mag enkel organisatorisch opzij of omhoog worden gedelegeerd aan medewerkers van het Kadaster, bijvoorbeeld in geval van tijdelijke of langdurige afwezigheid van een goedkeurder. Afhankelijk van de condities gesteld door de diensteigenaar kunnen additionele goedkeurders van toepassing zijn, zoals een aangewezen persoon die goedkeurt na controle van beschikbare licenties, uitvoering van verplichte opleidingen, et cetera.

5.2.1 Periodieke controle van toegekende toegangsrechten

Toegangsrechten worden minimaal jaarlijks, of bij grote wijzigingen beoordeeld door de verantwoordelijken die bij de oorspronkelijke aanvraag een beoordeling moesten geven. Kritieke toegangsrechten worden elk kwartaal herzien door dezelfde verantwoordelijken. Deze controles waarborgen dat toegangsrechten juist, volledig en in lijn met het beleid blijven.
Wanneer rechten niet tijdig worden gecontroleerd door de verantwoordelijke, worden na twee signaleringen[2] (met telkens vier weken tussenruimte) niet-geaccordeerde rechten ingetrokken door de LTB-desk[3]. Dit proces is zodanig ingericht dat rechten zorgvuldig worden ingetrokken en snel hersteld kunnen worden na akkoord van de verantwoordelijke.

5.2.2 Logging en monitoring

Alle goedkeuringen en afwijzingen uitgevoerd in het LTB-systeem worden gelogd, inclusief tijdstip van beoordeling en beoordelaar. Alle toewijzingen, wijzigingen en intrekkingen zoals bepaald in het LTB-systeem

[2] Hierbij kan tevens een risk- of security officer geïnformeerd worden.
[3] Sinds 14 oktober 2024 is de manager DPI Bedrijfsvoering door het bestuur bevoegd om autorisaties in te trekken.

worden vastgelegd, inclusief tijdstip en aanleiding, zoals handmatige actie, voortvloeiend uit een geautomatiseerde regel, etc.

5.3 Wijzigingen in accounts en bijbehorende permissies

5.3.1 Geautomatiseerde verwerking

Opdrachten van het LTB-systeem aan diensten worden bij voorkeur geautomatiseerd verwerkt, zodat wijzigingen in accounts en bijbehorende permissies plaatsvindt zonder handmatige tussenkomst[4]. Dit verhoogt de snelheid en nauwkeurigheid van de wijzigingen.
Omdat alle procescontroles in het LTB-systeem plaatsvinden, is het essentieel dat minimaal eens per kwartaal de toegangsrechten in het LTB-systeem vergeleken worden met de administraties van accounts en permissies in diensten.

5.3.2 Logging en monitoring

Beveiligingswaarschuwingen met betrekking tot het beheer van toegangsrechten worden geregistreerd, gemonitord, geanalyseerd en hersteld. Lessons learned worden toegepast om herhaling te voorkomen.

5.4 Toegang via Leveranciersportaal

Voor leveranciers die zelf bepalen welke medewerkers worden ingezet, biedt het LTB-systeem een Leveranciersportaal. Hier kunnen leveranciers toegangsrechten beheren die nodig zijn om de dienst te leveren die door Kadaster is afgenomen. De verantwoordelijke persoon van de leverancier bepaalt welke medewerker toegang nodig heeft. De Kadaster contracteigenaar, in overleg met de diensteigenaren en de verantwoordelijke persoon van de leverancier, bepaalt welke toegangsrechten nodig zijn voor het uitvoeren van de werkzaamheden.

Voorwaarden voor toegang:

- toegang is beperkt tot wat nodig is voor de uitvoering van de overeenkomst, waarin ook de contractuele afspraken over voldoen aan Kadaster security- en privacy beleid zijn overeengekomen[5];
- toegangsrechten voor leveranciersmedewerkers worden alleen toegekend binnen de condities gesteld door de diensteigenaren;
- leveranciers hebben geen toegang tot gegevens van het Kadaster, tenzij dit essentieel en uitlegbaar is. In dat geval wordt toegang geregeld via het Leveranciersportaal.
    - Bijvoorbeeld: Medewerkers van de leverancier die de uitbestede werkplek beheren hebben geen toegang tot gegevens van Kadaster opgeslagen in SharePoint gedeelde schijven.
    - Bijvoorbeeld: Medewerkers van de leverancier die security monitoring uitvoeren, hebben enkel toegang voor zover deze via het LTB-systeem, bij voorkeur via het Leveranciersportaal, is toegekend.

[4] Dus geautomatiseerde verwerking en handmatige verwerking (resp. Eng. automated provisioning en manual provisioning)
[5] Zie standaard IB bij contracten leveranciers

6 Authenticatie

6.1 Authenticatie vereisten

Authenticatie is een essentiële beveiligingsmaatregel die Kadaster in staat stelt te verifiëren of een gebruiker is wie hij/zij beweert te zijn. Dit, in combinatie met logging, maakt het gebruik van accounts herleidbaar naar een natuurlijke persoon. Alle digitale toegang tot producten, diensten, gegevens en bedrijfsmiddelen is beveiligd met multi-factor authenticatie (MFA).

Toegang voor medewerkers en gelijkgestelden verloopt via de centrale interne Single Sign-On (SSO)-voorziening.
Deze systemen waarborgen dat authenticatiegegevens, zoals wachtwoorden, voldoen aan de geldende eisen. Gebruikers moeten worden gewezen op hun verantwoordelijkheden, zoals het veilig opslaan en geheimhouden van authenticatiegegevens.
Diensteigenaren zijn verantwoordelijk voor aanvullende eisen bij specifieke situaties, zoals onpersoonlijke accounts of accounts met kritieke toegang.

6.2 Toegang en authenticatie van bedrijfsmiddelen

Vaste en extern ingehuurde medewerkers krijgen alleen toegang tot producten, diensten en gegevens van Kadaster via door Kadaster geauthentiseerde en compliant bedrijfsmiddelen. Gebruikers van eigen apparaten (Bring Your Own Device, BYOD) hebben uitsluitend toegang tot een niet-vertrouwd netwerk dat enkel publieke internettoegang biedt. BYOD-apparaten worden als inherent onveilig beschouwd.

Leveranciers mogen toegang krijgen tot Kadaster producten, diensten en gegevens vanaf niet door Kadaster verworven bedrijfsmiddelen, mits hierover afspraken zijn gemaakt. Deze afspraken omvatten authenticatie- en compliance-eisen voor de apparatuur die toegang biedt tot Kadaster producten, diensten en gegevens.

6.3 Reguliere gebruikersaccounts

Reguliere gebruikersaccounts moeten vanwege interoperabiliteit altijd beveiligd zijn met een wachtwoord. Voor toegang tot niet-publieke producten, diensten en gegevens van Kadaster is multi-factor authenticatie (MFA) verplicht.

6.3.1 Eisen voor authenticatiemethoden

MFA vereist een combinatie van:

- iets dat je bent (bijvoorbeeld vingerafdruk);
- iets dat je weet (bijvoorbeeld wachtwoord of pin);
- iets dat je hebt (bijvoorbeeld een hardware-token).

Beschikbare verificatieopties zijn:

- verificatie via een TOTP-app, zoals Microsoft Authenticator;
- verificatie via hardware met cryptografisch materiaal (FIDO2[6]-compatibel).

[6] FIDO2 is de overkoepelende naam voor de combinatie van de standaarden Client to Authenticator Protocols (CTAP) van de FIDO Alliance en Web Authentication (WebAuthn) van het W3C.

6.3.2 Eisen voor authenticatiegegevens

Authenticatiegegevens omvatten wachtwoorden, pincodes of andere toegangsmiddelen. De eisen die worden gesteld aan authenticatiegegevens zijn weergegeven in tabel 3.

Eis		Gebruikersaccount
Wachtwoord	Lengte	Minimaal 12 karakters
	Wijze van totstandkoming	Door gebruiker opgegeven
	Wachtwoordhistorie	Nee
	Complexiteitseis	Ja
	Verbod op gebruik van woorden op lijst van gelekte en/of veel voorkomende wachtwoorden	Ja
	Lock-out	Na 5 foutieve pogingen
	Lock-out periode	15 minuten
	Wachtwoordleeftijd	Geldig totdat er tekenen zijn van diefstal
	Scherm lock	Na 15 minuten inactiviteit
Extra verificatie *[7]	Geldigheid (compliant device)	7 dagen
Pincode (mobiel & FIDO2)	Aantal tekens	Minimaal 6 tekens

Tabel 1 – Eisen voor authenticatiegegevens van reguliere gebruikersaccounts

6.3.3 Uitgifte wachtwoorden aan gebruikers

Het beheer van geheime authenticatie-informatie moet voldoen aan de volgende regels:

- als er twijfel bestaat over de geheimhouding van een wachtwoord, moet de medewerker het wachtwoord direct wijzigen;
- wachtwoorden mogen uitsluitend bekend zijn bij de beoogde medewerker en niet met anderen worden gedeeld;
- initiële wachtwoorden moeten binnen twee werkdagen worden gewijzigd; gebeurt dit niet, dan wordt het account geblokkeerd;
- wachtwoorden worden op een veilige manier uitgegeven, waarbij de identiteit van de ontvanger wordt gecontroleerd.

6.4 Onpersoonlijke accounts

Diensteigenaren zijn verantwoordelijk voor maatregelen om authenticatiegegevens van onpersoonlijke accounts geheim te houden. De volgende eisen zijn van toepassing voor deze accounts:

- de bedrijfsreden voor het bestaan van het account wordt vastgelegd;
- wanneer het technisch mogelijk is om het account te verwijderen en het account niet langer nodig is, dan wordt deze binnen één maand verwijderd;
- gebruik van het account is beperkt tot een geautoriseerd systeem, service of applicatie;
- gebruik van het account is enkel mogelijk vanaf een beperkte lijst van IP-adressen.

[7] Binnen Kadaster wordt gebruik gemaakt van OAuth2.0. Toelichting en instellingen: https://www.forumstandaardisatie.nl/open-standaarden/nl-gov-assurance-profile-oauth-20

6.4.1 Eisen ten aanzien van authenticatiegegevens

Eis		Onpersoonlijk account
Wachtwoord	Lengte	32 karakters, of minimaal 20 karakters
	Wijze van totstandkoming	Automatisch en willekeurig gegenereerd[8]
	Wachtwoordleeftijd	Maximaal 6 maanden

Tabel 2 - Eisen voor authenticatiegegevens van onpersoonlijke accounts

6.4.1.1 Voor gebruik door codes

Voor systeem-, service-, en applicatie accounts zijn aanvullende eisen opgenomen om de verstoringen van de processen zoveel mogelijk te voorkomen. De volgende aanvullende eisen worden gesteld aan dit type accounts:

- geen hergebruik van wachtwoorden. Elk wachtwoord moet uniek zijn;
- authenticatiegegevens mogen niet in de broncode worden opgenomen. Gebruik hiervoor bijvoorbeeld injectie via omgevingsvariabelen.

6.4.1.2 Voor noodherstel

Het wachtwoord voldoet aan de complexiteitseisen van een privileged account, met uitzondering dat deze niet gebonden is aan een levensduur. Het wachtwoord dient als een eenmalig wachtwoord (One-Time Password, OTP) en moet na elk gebruik worden gewijzigd.

6.4.2 Logging en monitoring

Beveiligingswaarschuwingen met betrekking tot onpersoonlijke accounts worden geregistreerd, gemonitord, geanalyseerd en hersteld via centrale security monitoring. Dit omvat minimaal waarschuwingen over het beheer van onpersoonlijke accounts, zoals het aanmaken en wijzigen van permissies, evenals afwijkende activiteiten van deze accounts, bijvoorbeeld op basis van IP-adres, datum of tijdstip. Om herhaling te voorkomen, worden lessen getrokken uit incidenten.

6.5 Accounts met kritieke toegang

De diensteigenaar is verantwoordelijk voor aanvullende beveiligingsmaatregelen op accounts met kritieke toegang, zoals het monitoren en/of opnemen van gebruik ervan en het geheim houden van de inloggegevens (wachtwoorden, private keys en tokens).

Eis		Account met kritieke toegang
Wachtwoord	Lengte	Minimaal 20 karakters
	Wijze van totstandkoming	Automatisch en willekeurig gegenereerd
	Wachtwoordleeftijd	Maximaal 3 maanden

Tabel 3 - Eisen voor authenticatiegegevens van accounts met kritieke toegang

Diensteigenaren dienen ervoor te zorgen dat gebruik van accounts door een natuurlijk persoon altijd herleidbaar is. Dit betekent dat default accounts waar mogelijk worden gedeactiveerd. Als dit niet mogelijk is, worden deze accounts ontsloten via de centrale PAM voorziening. Hierdoor is het gebruik van dit type accounts herleidbaar. Dit geldt uitdrukkelijk ook voor:

[8] Minimaal 60 bit entropie, bijv. te controleren in Keepass

- default accounts die standaard zijn ingebouwd in applicaties/systemen;
- onpersoonlijke accounts waarbij men weet of redelijkerwijs kan vermoeden dat de eigenaar niet de gebruiker van het account is (generieke accounts, beheeraccounts, etc.).

Regels voor het gebruik van accounts met kritieke toegang:

- er is te allen tijde een bijgewerkt inschrijfregister aanwezig met details over wie, wanneer het account gebruikt heeft;
- alleen natuurlijke personen mogen inloggen in deze accounts, en alleen als zij zijn ingeschreven in het register;
- in het geval van toegang tot applicaties/systemen die onderdeel zijn van een dienst geclassificeerd als Hoog of als onderdeel van het kernlandschap geldt:
    - Bij het inschrijven in het logboek moet worden opgegeven welke activiteiten worden uitgevoerd;
    - Indien van toepassing moet een verwijzing naar een openstaand incident worden opgenomen;
- de diensteigenaar kan vooraf bepalen dat expliciete goedkeuring nodig is van een verantwoordelijke, zoals een lijnmanager, risk officer of incidentmanager;
- de diensteigenaar bepaalt voorafgaand aan gebruik een beperking voor de duur van gebruik, met een maximum van 10 uur. Een langere gebruiksduur is alleen mogelijk, indien voorafgaand aan het verstrijken van het maximum van 10 uur expliciete goedkeuring hiervoor gegeven is door een verantwoordelijk persoon voorafgaand aangewezen door de diensteigenaar, zoals een lijnmanager, risk officer of incidentmanager inclusief vermelding van de activiteiten en eventuele incidentverwijzingen;
- authenticatiegegevens blijven waar mogelijk geheim en worden na gebruik ongeldig gemaakt;
- opslag van wachtwoorden is alleen versleuteld toegestaan in de goedgekeurde PAM-oplossing. De wachtwoorden worden elk kwartaal gewijzigd.

6.5.1 Logging en monitoring

Beveiligingswaarschuwingen met betrekking tot accounts met kritieke toegang worden door de centrale security monitoring geregistreerd, gemonitord, geanalyseerd en, indien nodig, hersteld. Aanvullend op de eerder gestelde logging-eisen voor onpersoonlijke accounts, omvat dit minimaal beveiligingswaarschuwingen over afwijkende activiteiten van accounts met kritieke toegang ten opzichte van gebeurtenissen geregistreerd in de PAM oplossing, zoals ingebruikname via PAM en vastgelegde IP-adressen van gebruikers.
Ter voorkoming van herhaling wordt er lering uit getrokken.

7 Bijlagen

Begrippen en definities

Begrip	Uitleg
API	Application Programming Interface is een combinatie van technische bestanden, documentatie en andere ondersteuning die helpt bij het aanroepen van externe applicaties. Een API wordt gepubliceerd door de softwareontwikkelaar zodat andere ontwikkelaars weten hoe de software te koppelen aan de eigen software. Het is daarmee geen standaard, maar meer een handleiding die kan worden gebruikt van een machine tot machinekoppeling.
Applicatie	Automatisering die wordt gebruikt in een dienst voor het invoeren, verwerken, opslaan en uitvoeren van informatie.
Applicatie eigenaar	Synoniem voor diensteigenaar
Authentiseren / Authenticatie	Authenticatie is het proces waarbij wordt nagegaan of de gepresenteerde identiteit dezelfde persoon is als tijdens de eerdere verificatie. Welk middel wordt gebruikt is weer afhankelijk van de betrouwbaarheid die voor een bepaalde service nodig is.
Autorisatiecontrole	Proces van uitoefenen van autorisaties (toegangsrecht) door het subject. (Real time proces voor toestaan of weigeren van het toegangsrecht.)
Autorisatiematrix	Matrix waarin is weergegeven welk subject, via welke rol geautoriseerd is voor welke applicatiefunctie of informatie
Autorisatiemodel	Een vereenvoudigde weergave van de werkelijkheid. Beschrijft hierdoor slechts de samenhang tussen de verschillende autorisaties
Autoriseren / Autorisatie	Autorisatie is enerzijds het proces van het beheer van toegangsrechten. Dit vindt plaats op het Logische Toegang Beveiliging Systeem (LTBS) en bevat de regels voor objecten en subjecten voor het beheer van toegangsrechten. Anderzijds is dit het proces waarin een subject (een persoon of een proces) toegangsrechten verkrijgt op het benaderen van een object (een bestand, een systeem). Dit vindt plaats op het object zelf, op basis van de regels van het LTBS.
Bring Your own Device (BYOD)	BYOD (of kortweg BYO) is een bedrijfsconcept waarbij personeel apparatuur naar werk meebrengt die niet wordt uitgeleverd door de werkgever. Vaak wordt bij deze trend gerefereerd naar het meebrengen van mobiele apparatuur, zoals laptops, tablets en smartphones, maar het kan ook gaan om complete desktopcomputers die zakelijk gebruikt worden maar door de werknemer betaald zijn.
Bron	De oorsprong van de benodigde informatie.
Cloud	Het opslaan en opvragen van gegevens, software en bestanden op een andere plek dan uw eigen locatie. Omdat deze opslagplek vaak niet zichtbaar en onbekend is, wordt de term cloud, ofwel wolk, gebruikt. Het werken in de cloud gebeurt meestal via het internet.
Controlemodel	Een vereenvoudigde schematische weergave van de werkelijkheid. Beschrijft hierdoor slechts de samenhang tussen de verschillende controles
Database	Gegevensbank; het is een systeem voor de opslag van gegevens. Een database is opgebouwd uit tabellen die bestaan uit records(regels) die zijn gevuld met data.

Begrip	Uitleg
Data eigenaar	De data eigenaar is de aangewezen eigenaar, en dus eindverantwoordelijk voor de data in of buiten de applicatie. - Voor wat betreft LTB bepaalt de data eigenaar wie toegang krijgt tot zijn/ haar data. - Voor data in een applicatie is de data eigenaar eindverantwoordelijk voor het bestaan, de inhoud, onderhoud en beheer van de data autorisatiematrix. De eigenaar stelt deze op in samenwerking met de applicatie eigenaar en functioneel beheerder. - Voor data in gedeelde mappen, folders of andere schijven is de data eigenaar verantwoordelijk voor het bestaan, de inhoud, onderhoud en beheer van een mappen autorisatiematrix. - Daarnaast ziet hij/zij toe op een juiste uitvoering van het toegangsbeheer door de toegangsbeheerder. De data eigenaar is in principe een manager in de laag direct onder de directieraad. Voor projectdata geldt dat de projectleider de data eigenaar is. - De data eigenaar is eveneens verantwoordelijk voor de risico's die gemoeid gaan met zijn of haar data. Daarmee is de data-eigenaar ook risico-eigenaar (risk owner). - Data eigenaarschap speelt met name bij applicaties zoals SAP BW, AKR/HYP en ongestructureerde data (bijv. U: schijf, gedeelde folders).
Default account	Nodig voor het functioneren van het systeem; accounts die standaard meekomen als je een product koopt. Bijvoorbeeld Windows administrator en Linux Root. Deze zijn standaard aanwezig.
Dienst eigenaar	De diensteigenaar is vastgelegd in de CMDB. - Is de aangewezen eigenaar, en dus eindverantwoordelijke voor de dienst en onderliggende applicatie en systemen. Voor wat betreft LTB is de diensteigenaar eindverantwoordelijk voor het bestaan, de inhoud, onderhoud en beheer van de condities voor toegang tot de dienst, applicatie en systeem. De eigenaar stelt deze op in samenwerking met functioneel beheer en/of data eigenaar/ eigenaren. - Daarnaast ziet de diensteigenaar toe op een juiste uitvoering van het toegangsbeheer. - De diensteigenaar is in veel gevallen ook de data-eigenaar. - De diensteigenaar is eveneens verantwoordelijk voor de risico's die gemoeid gaan met de dienst, applicatie en systeem en is daarmee ook risico-eigenaar (risk owner).
Gebruiker account	Gebruiker accounts zijn accounts met reguliere rechten, i.e. zonder speciale vergaande toegangsrechten.
Generiek account	Generieke accounts zijn niet-persoonlijke accounts.
Identificeren / Identificatie	Identificatie is het presenteren van een identiteit aan een systeem. Verificatie van de identiteit is het proces dat plaatsvindt bij de registratie van de identiteit, bijvoorbeeld in een HR-bronsysteem, en waarbij een digitaal identiteitsbewijs wordt uitgegeven. Hiermee is de digitale identiteit gelinkt aan een persoon. Verificatie van de identiteit vindt ook plaats bij de uitgifte van digitale identiteitsbewijzen door externe Identity Providers (zoals DigiD, eHerkenning) en is afhankelijk van de vereiste betrouwbaarheid van het digitale identiteitsbewijs.
Identiteit	Een identiteit is het geheel aan kenmerken dat een persoon of andere entiteit uniek herkenbaar maakt
KEA	Kadaster Enterprise Architectuur is een coherente, consistente verzameling principes, verbijzonderd naar uitgangspunten, regels, richtlijnen en standaarden – soms vastgelegd in patterns – die beschrijft hoe het Kadaster, de informatievoorziening, de applicaties en de infrastructuur hun vorm hebben gekregen en hoe zij zich voordoen in het gebruik.
Leverancier	Een leverancier levert goederen of diensten in ruil voor geld. De leverancier is verantwoordelijk voor de aansturing van zijn eigen medewerkers. In een contract wordt de identiteit (KVK nr.) van de leverancier en de afspraken vastgelegd over de te leveren dienst of product inclusief de randvoorwaarden.
Logging en monitoring	Logging en monitoring is het proces van (real-time) analyseren en herstellen van, en lering trekken uit beveiligingswaarschuwingen op het gebied van beheren van toegangsrechten.

Begrip	Uitleg
Medewerker	Natuurlijke personen die op basis van een aanstelling, contract of overeenkomst bij het Kadaster werken. Dit betreffen zowel eigen medewerkers als ingehuurde medewerkers.
Objecten	Entiteit die de handeling ondergaat van een subject. Voorbeelden van objecten zijn producten, diensten en bedrijfsmiddelen (systemen, applicaties en databases).
Privilege account	Privilege accounts zijn accounts met speciale, vergaande toegangsrechten. Dit zijn o.a.: • Default beheeraccounts. Nodig voor het functioneren van het systeem, bijvoorbeeld Windows administrator en Linux Root. Deze zijn standaard aanwezig. • Gepersonaliseerde beheeraccounts. Nodig voor het beheren van een applicatie, systeem of database (database administrator (DBA). Deze worden door een beheerder aangemaakt, de benodigde rechten worden gekoppeld aan het gebruikersaccount. • Applicatie-, service- en systeemaccounts. Gebruikt door applicaties, (systeem)processen of het besturingssysteem. Bijvoorbeeld system-to-system accounts of een account dat gebruikt wordt door een applicatie om een database te benaderen. Deze zijn standaard aanwezig of worden door een beheerder aangemaakt. Systeemprocessen draaien onder een eigen gebruikersnaam, voor zover deze processen handelingen verrichten voor andere systemen of gebruikers. • Gebruikersaccounts die een verhoogd risico op de beschikbaarheid, vertrouwelijkheid of integriteit van informatie kunnen geven. Bijvoorbeeld een account van een hoofdbewaarder of een account van een functioneel beheerder van een applicatie.
Product of dienst	Waar in dit document gesproken wordt over producten/diensten worden elektronische producten/diensten bedoeld die uitsluitend voor klanten zijn bestemd.
RACI tabel	Tabel die gehanteerd wordt om de rollen en verantwoordelijkheden van de personen die bij LTB werkzaamheden betrokken zijn weer te geven. De Nederlandse aanduiding is VERI-Matrix wat staat voor Verantwoordelijk / Eindverantwoordelijk / Raadplegen / Informeren.
Rollenmodel	Een vereenvoudigde weergave van de werkelijkheid. Beschrijft hierdoor slechts de samenhang tussen de verschillende rollen.
SA-LTB	Solution architectuur Logische toegangsbeveiliging (SA-LTB) is het essentiële ontwerp gebaseerd op principes, modellen en standaarden van het LTB informatiesysteem en zijn effectieve inzetbaarheid in een operationele Kadasteromgeving met als doel het oplossen van de verschillende LTB business problemen en behoeften.
Secrets	Alle vertrouwelijke authenticatie informatie behorende bij een account (bijv. wachtwoorden, keys of tokens)
Subjecten	Entiteit die een handeling uitvoert op een object. Het subject kan een identiteit, gebruiker of account zijn (ook van een informatiesysteem). Voorbeelden van subjecten zijn medewerkers, leveranciers, kandidaten en gasten.
Systeem	Geautomatiseerd object dat als basis dient voor bijvoorbeeld een applicatie of database. (Bijvoorbeeld Windows Active Directory.)
Systeemeigenaar	Synoniem voor diensteigenaar.
Toegangsbeheerder	• Is verantwoordelijk voor het opvoeren, wijzigen en verwijderen van toegangsrechten tot applicaties aan een gebruiker (account). • Daarnaast verantwoordelijk voor het in gang zetten van beoordelingsprocessen. Hij legt periodiek, in opdracht van de applicatie-eigenaar, een lijst met gebruikers en hun toegangsrechten voor aan de lijnmanager met de vraag of de toegang nog benodigd en/of correct is. • Bovenstaande gebeurt op basis van de voorgeschreven procedures en de autorisatiematrix (beschreven in dit document).
Toegangsrecht	De wijze waarop een tot toegang bevoegd gebruiker met een beschermd(e) bestand of functionaliteit mag omgaan. (Bijvoorbeeld alleen lezen of lezen en schrijven, etc.).

Handvatten ten aanzien van bronsystemen

Bronsysteem eigen- en ingehuurde medewerkers
Wil een bronsysteem een gezaghebbend bronsysteem (authoritative source) voor identiteiten van eigen – en ingehuurde medewerkers zijn, dan kunnen de volgende aspecten gehanteerd worden:

- De verantwoordelijkheid voor de actualiteit, juistheid en volledigheid van de gegevens zijn belegd bij de proceseigenaar van in dienst- , wijziging van- en uitdiensttreding van eigen – en ingehuurde medewerkers. Dientengevolge komen in het LTB-systeem alleen digitale identiteiten van eigen – en ingehuurde medewerkers voor die in het bronsysteem aanwezig zijn.
- Een geautomatiseerde koppeling tussen bronsysteem en LTB-systeem is gewenst ten behoeve van het kunnen aanmaken van het account voor de eerste werkdag, en het verwijderen van het account op de laatste werkdag.
- De identiteitsgegevens moeten juist zijn. De identiteit moet zijn geverifieerd
- Alleen die identificerende gegevens worden opgeslagen in het bronsysteem en gedeeld met het LTB-systeem die benodigd zijn voor het beoogde doel.
- De identiteitsgegevens moeten volledig zijn ten behoeve van het doel toegangscontrole. Om volledig te kunnen functioneren, dient het LTB-systeem voor dit doel tenminste de volgende gegevens van alle identiteiten van het bronsysteem te ontvangen:
    - aanstellingen
    - voornaam, achternaam, tussenvoegsel;
    - functie;
    - e-mailadres;
    - naam afdeling;
    - naam direct leidinggevende;
    - personeelsnummer of vergelijkbaar.

Bronsysteem leveranciers
Wil een bronsysteem als gezaghebbend bronsysteem (authoritive source) voor leveranciers dienen, dan kunnen de volgende aspecten gehanteerd worden:

- De verantwoordelijkheid voor de actualiteit, juistheid en volledigheid van de gegevens is belegd bij de proceseigenaar van het opnemen, wijzigen en verwijderen van leveranciers. Dientengevolge komen in het LTB-systeem alleen leveranciers voor die in het bronsysteem aanwezig zijn.
- Real-time koppeling tussen bronsysteem en LTB-systeem is vereist t.b.v. het kunnen aanmaken van het account op de dag van aangaan van de overeenkomst, en het verwijderen van het account op de dag van het ontbinden van de overeenkomst.
- De identiteitsgegevens moeten juist zijn. De identiteit moet zijn geverifieerd
- Alleen die identificerende gegevens worden opgeslagen in het bronsysteem en gedeeld met het LTB-systeem die benodigd zijn voor het beoogde doel.
- De identiteitsgegevens moeten volledig zijn ten behoeve van het doel toegangscontrole. Om volledig te kunnen functioneren, dient het LTB-systeem de volgende gegevens te ontvangen van het bronsysteem:

- voornaam, achternaam, tussenvoegsel;
- bedrijfsnaam leveranciers;
- e-mailadres;
- naam geleverde dienst;
- KvK-nummer leverancier (unieke identifier);
- OIN (Organisatie-identificatienummer) voor overheidsinstanties (unieke identifier). Organisaties die met of binnen de overheid digitaal informatie willen uitwisselen op basis van de Digikoppeling Standaard kunnen een OIN krijgen. Dit is een uniek identificerend nummer dat gebruikt wordt in de digitale communicatie en onder meer wordt opgenomen in PKI-certificaten.

Welke identiteitsgegevens nodig zijn is afhankelijk van het proces of de dienst en moet o.b.v. een risicoanalyse worden vastgesteld.