

Algemene informatie

Aanbesteding: Implementation, Hosting, Maintenance and Support of Midpoint
Aanbestedende Dienst: Fontys Hogeschool
Referentie: -

Toelichting:

Vraag en antwoord

Ref.nr. **Onderwerp:**
1 Q/A chapter 4.1 in RFP

Vraag:

In chapter 4.1 of the steps involved in selection and award, can you detail the specific knock-out criteria in the five steps:

1. Review to verify proper form, structure and timeliness (knock-out criteria) (Chapter 5) and quality of the Bidder (knock-out criteria) (chapter 6).
2. Review in connection with Grounds for Exclusion and Suitability Requirements (knock-out criteria) (Chapter 7).
3. Review based on the Schedule of (minimum) Requirements (knock-out criteria) (Chapter 8).
4. Evaluation based on Award criteria (Chapter 9).
5. Intention to award and final award

Antwoord:

The knock-out criteria in Chapter 4.1 correspond directly to the minimum requirements set out in the Tender Document. For clarity, the five steps involve the following:

Step 1 – Form, structure, timeliness & quality (Chapters 5 and 6)

Criteria relating to correct submission of the Bid (format, completeness, signatures) and the organizational quality requirements applicable to the Bidder.

Step 2 – Grounds for Exclusion & Suitability Requirements (Chapter 7)

Criteria arising from the ESPD in connection with:

- Grounds for Exclusion, and
- Suitability Requirements (insurance, references, information security, and registration in a professional or trade register).

The Bidder declares compliance via the ESPD, reference statement and an extract (or copy of an extract) from the professional or trade register of the country in which they have their registered offices.

Step 3 – Schedule of (minimum) Requirements (Chapter 8)

The requirements that must be met in full. By submitting a Bid, the Bidder

confirms unconditional compliance.

Step 4 – Award criteria (Chapter 9)

Evaluation of qualitative criteria. Sub-criteria with a minimum threshold must meet that threshold; Bids scoring below the required minimum will not be evaluated further.

Step 5 – Intention to award and final award

No additional criteria apply. The highest-ranked Bidder proceeds. During this step, the contracting authority will request the required supporting documents from the highest-ranked Bidder. In addition, a verification meeting will be held to confirm the correctness and completeness of the submitted Bid and to clarify any outstanding points.

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen:

P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op:

12 dec 2025

Ref.nr.

2

Onderwerp:

EA: Implementation, Hosting, Maintenance and Support of Midpoint

Vraag:

Naar aanleiding van onze evaluatie van uw aanbesteding voor de MidPoint als IGA-oplossing adviseren wij om de keuze voor MidPoint los te laten in deze aanbesteding.

Hierbij onze onderbouwing:

- Ontbreken van opensource governance en verhoogde supply-chain risico's
Geen onafhankelijke governance, beperkte kwaliteitscontrole en sterke afhankelijkheid van een kleine groep maintainers.
- Geen geborgd support- en verantwoordingsmodel
Onzekerheden rondom verantwoordelijkheid bij security-issues, SLA's voor patches en omgang met breaking changes.
- Continuïteitsrisico bij vendor
Beperkte organisatieomvang en afhankelijkheid van één leverancier
vergroten risico's bij uitval of overname.
- Zeer beperkte community-adoptie en externe code-validatie

Lage aantallen forks, contributors en onafhankelijke audits in vergelijking met volwassen opensource-projecten.
Gezien deze risico's adviseren wij te focussen op volwassen, commercieel gedragen en breed geadopteerde alternatieven zoals SailPoint (SaaS/on-prem), HelloID, Microsoft Entra Governance of Okta Governance.
Onze vraag aan Fontys: Wij begrijpen dat het loslaten van Midpoint een grote impact heeft op deze aanbesteding, maar wij vragen u toch om inchrijvers de mogelijkheid te bieden om zich niet alleen te beperken tot MidPoint en de focus te richten op de genoemde alternatieven? Bent u bereid dit aan te passen en uw motivatie hierop toe te lichten?

Antwoord:

Fontys appreciates your feedback. However Fontys will not adjust the scope of the tender. The choice for MidPoint is a deliberate and strategically motivated decision that precedes this procurement procedure. The tender therefore focuses on the implementation, hosting, maintenance, support and training of the MidPoint solution—not on a comparative product selection.

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen: P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op: 12 dec 2025

Ref.nr.

5

Onderwerp:

Tender Document, requirement 5

Vraag:

The “Documentation for Service Providers” mentioned in chapter 8.1, requirement 5 cannot be found. Is there any other valid link to be used for evaluating the service provider's documentation for federated authentication?

Antwoord:

The mentioned location is incorrect. You can find the current information at the following location: <https://servicedesk.surf.nl/wiki/spaces/IAM/pages/128909810/SURFconext+for+Service+Providers>

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen: P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op: 12 dec 2025

Ref.nr.

6

Onderwerp:

Tender Document, requirement 12

Vraag:

The retention policy mentioned in 8.1, requirement 12 cannot be found using the provided URL. Is there any other valid link to be used for evaluating the retention periods?

Antwoord:

The mentioned location is incorrect. The functional design will define the retention periods that apply to the Midpoint solution and the personal data. The contractor's retention regime will comply at all times with the retention periods stated in the functional design.

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen: P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op: 12 dec 2025

Ref.nr.

7

Onderwerp:

Tender Document, 3.1.7 Data migration

Vraag:

Could you clarify what is meant by “historical data” as mentioned in 3.1.7 within the functional points of attention? Does this include only “historical” identity data such as inactive, not yet deleted identities and their connection to not yet deleted user accounts and not yet removed entitlements or does this also cover already removed but archived entitlement assignment, historical attribute changes and such “historical data”?

Antwoord:

By "historical data" as mentioned in 3.1.7 (Data migration), we only refer to previously issued identities (PCN) with natural person holder information to which the identity belongs. We use the policy that when a natural person returns in the future, the person will receive the initial identity (PCN).

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen:

P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op:

12 dec 2025

Ref.nr.

8

Onderwerp:

Tender Document, Bid

Vraag:

Are documents required to bear handwritten signatures, and if so, which ones?

Antwoord:

Digital (or handwritten). The following documents must be signed:

- '- Appendix A ESPD
- '- Appendix B Reference statement
- '- Appendix C Price sheet

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen: P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op: 12 dec 2025

Ref.nr.

9

Onderwerp:

Tender Document, 3.1.3.3 and Agreement 2.3

Vraag:

Are we correct in assuming that the timely achievement of the milestone for Phase II is no longer the sole responsibility of the bidder, provided that Fontys or a third party designated by Fontys participates in the implementation of the milestone for Phase II and its implementation cannot be controlled by the bidder?

Antwoord:

Fontys confirms that the Contractor remains responsible for delivering Phase 2 in accordance with the agreed scope, planning and milestones to the extent that the activities fall within the Contractor's control.

As stated in the Tender Document (section 3.1.3.3) and the Agreement (article 3.2), Fontys may decide to develop certain interfaces itself or have them developed by a third party. In such cases, the Contractor is not responsible for delays or non-achievement of the Phase 2 milestone that are attributable to activities performed by Fontys or third parties designated by Fontys.

The overall milestone (Ready-to-Use Delivery Phase 2) remains applicable, but the Contractor will not be held responsible for elements outside its reasonable sphere of influence.

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen: P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op: 12 dec 2025

Ref.nr.
10

Onderwerp:
Tender Document, requirement 33

Vraag:
Are we correct in assuming that the application of Fontys' corporate identity simply means the use of colors, fonts, and logos?

Antwoord:
Yes, this is correct.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:
Vragenronde 1

Percelen: P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op: 12 dec 2025

Ref.nr.
11

Onderwerp:
Tender Document, 3.1.5

Vraag:
Are we correct in assuming that “the contractor will review and accept the functional design” in the means of 3.1.5 also includes remediation on the functional design by Fontys based on the contractor’s review?

Antwoord:
The assumption that was made is correct.

Fase:
Inschrijffase

Inschrijfronde:
Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen: P1 Implementation, Hosting, Maintenance and Support of Midpoint**Beantwoord op:** 12 dec 2025**Ref.nr.**

12

Onderwerp:

Tender Document, requirement 16

Vraag:

Requirement [16]: E-Mail Security

The specified email security standards (DMARC, DKIM, SPF, STARTTLS, DNSSEC, DANE) are implemented at the mail transfer agent (MTA) and DNS infrastructure level, not within application software such as midPoint. MidPoint supports integration with any SMTP-compliant mail server, including those configured with TLS encryption. Are we correct in assuming that Fontys will provide a secured mail relay or SMTP infrastructure meeting the requested requirement to which the midPoint solution shall be integrated?

Antwoord:

In the long term, Fontys wishes to transition to its own solution for email security. At this moment, Fontys does not yet have such a solution. Bidders are therefore required to include the costs for this additional email service in their bid. The implementation costs must be included in the one-off costs for Phase 1. The recurring costs must be included in the periodic costs. These costs must be clearly traceable in the detailed price breakdown (to be added as Appendix D to the bid). When Fontys transitions to its own solution, these costs will be deducted.

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen: P1 Implementation, Hosting, Maintenance and Support of Midpoint**Beantwoord op:** 12 dec 2025

Ref.nr. 13
Onderwerp: Tender Document, requirement 17

Vraag:

Requirement [17]: DNSSEC

The specified DNS security is implemented at the DNS server level. As the midPoint solution will be integrated into the Fontys infrastructure via a site-to-site VPN, DNS resolution will take place within the Fontys DNS infrastructure. Are we correct in assuming that Fontys will provide DNS infrastructure capable of DNSSEC meeting the requested requirement to which the midPoint solution shall be integrated with?

Antwoord:

Yes, your assumption is correct.

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Perceelen: P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op: 12 dec 2025

Ref.nr. 14
Onderwerp: Tender Document

Vraag:

Are we correct in assuming that the described identity model results in one person being represented as multiple identities for multiple relationships (e.g. student, employee, lecturer) having different logins, passwords and entitlements as these will be created due to identity type specific business logic?

Antwoord:

In the current situation, if an employee is also a student, the person will receive one personal identity (PCN) as an employee and one personal identity (PCN) as a student. Since we are migrating AS-IS, this setup will remain in place. In the future, we may wish to change this to a single identity per natural person, but this is not within the current scope.

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen:

P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op:

12 dec 2025

Ref.nr.

15

Onderwerp:

Tender Document

Vraag:

Are we correct in assuming that both on-prem ADs (MS AD, EDS MS AD) are connected to MS Exchange Online for mailbox related use cases?

Antwoord:

No, only MS AD is connected to MS Exchange.

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen:

P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op:

12 dec 2025

Ref.nr.

16

Onderwerp:

Tender Document

Vraag:

Could you specify what kind of objects are currently managed by MIM in Entra ID and will need to be managed by midPoint after Phase 1?

Antwoord:

In the current situation, the MIM system is connected to MS AD, and MS AD is connected to MS Entra ID. With the Midpoint solution, we must be able to manage MS AD objects (as MIM currently does), but also at least user accounts and groups in Entra ID (cloud-only objects that are not synchronized with MS AD).

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Perceelen: P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op: 12 dec 2025

Ref.nr.

17

Onderwerp:

Tender Document

Vraag:

Are there any requirements for reporting or access recertification within the Functional Design for Phase 1?

Antwoord:

At this moment, the requirements for reporting are not yet defined. We will define them in the functional design.

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Perceelen: P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op: 12 dec 2025

Ref.nr.
18

Onderwerp:
Tender Document, notifications

Vraag:

Are notifications from midPoint (e.g. for current approval processes) expected via other channels than email, or can we assume that email-based notifications are sufficient to fulfil the requirements?

Antwoord:

At this moment email-based notifications are sufficient.

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen:

P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op: 12 dec 2025

Ref.nr.
19

Onderwerp:
Tender Document

Vraag:

Given the current implementation with MIM, how are initial passwords delivered to the affected user within the account creation process?

Antwoord:

For the user type Student, an email message is sent to his/her private email address. For the user type Employee, an email message is sent to the authorized person for transfer to the employee.

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen: P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op: 12 dec 2025

Ref.nr.

20

Onderwerp:

Tender Document

Vraag:

Can we assume that the CSV-based interface used for the source system connectivity towards HR2Day (Phase 1) is the same CSV-based interface for the target system connectivity towards HR2Day (Phase 2) or are these different CSV's

Antwoord:

Yes, this is the same CSV-based interface.

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen: P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op: 12 dec 2025

Ref.nr.

21

Onderwerp:

Tender Document

Vraag:

What approval processes are in place using MIM for access requests that will need to be replaced by midpoint?

Antwoord:

No, there are currently no access approvals defined in MIM.

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen:

P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op:

12 dec 2025

Ref.nr.

22

Onderwerp:

Tender Document

Vraag:

Will access request functionality be available for all identities being managed in MidPoint with the whole extend of access entitlements, or will there be limitations of requestable access entitlements per identity group?

Antwoord:

In principle, only per identity group.

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen:

P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op:

12 dec 2025

Ref.nr.

23

Onderwerp:

Tender Document

Vraag:

Are there any dashboards being implemented with MIM as of today that

need to be replaced by midPoint during Phase 1 or Phase 2?

Antwoord:

No.

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen:

P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op:

12 dec 2025

Ref.nr.

24

Onderwerp:

Appendix 3, Appendix 5; CRM next

Vraag:

As stated in Appendix 3, Relationship in source system CRM is not in project scope, while Appendix 5 lists Relationships in CRM-next as System to be interconnected. Could you clarify if CRM in the means of Appendix 3 is the same as CRM-next in the means of Appendix 5 and if it is in-scope or out-of-scope?

Antwoord:

In Appendix 3, the term CRM refers to CRM-next. The statement in Appendix 3 is incorrect. CRM-next is in scope as a combined source-target system. A single connector will be used for CRM-next: it will receive data from CRM-next and send the identity (PCN) back to CRM-next. Therefore, for implementation purposes, CRM-next is handled with one connector.

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen: P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op: 12 dec 2025

Ref.nr.
25

Onderwerp:
FAM

Vraag:

Could you clarify “non-personal identities” in the means of FAM?

Antwoord:

FAM stands for Functional Account Management and is used for the management of non-personal functional accounts. In this context, non-personal functional accounts are the same as non-personal identities.

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen: P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op: 12 dec 2025

Ref.nr.
26

Onderwerp:
Appendix 3, Fontys 06 number

Vraag:

Could you clarify what the “Fontys 06 number” is as mentioned in Appendix 3 with regard to the charging database?

Antwoord:

The term 'Fontys 06 number' refers to Dutch mobile phone numbers used by Fontys employees for multifactor authentication purposes (in the Netherlands, all mobile numbers start with 06).

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen: P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op: 12 dec 2025

Ref.nr.

27

Onderwerp:

Tender Document, 3.1.6

Vraag:

Are we correct in assuming that, once the contract has been awarded and the project has begun, Fontys will be willing to discuss individual interface adjustments with regard to the interface technology used for the source and target systems to be connected, provided that this would prove advantageous for the overall implementation?

Antwoord:

Yes, your assumption is correct. At this stage of the tender, Bidders must base their offer on the AS-IS interfaces as specified. Any potential adjustments can only be agreed upon after award.

Fase:

Inschrijffase

Inschrijfronde:

Inschrijfronde 1

Vragenronde:

Vragenronde 1

Percelen: P1 Implementation, Hosting, Maintenance and Support of Midpoint

Beantwoord op: 12 dec 2025