Application Integration Service Requirements

Deliverable D44.2

Document Identification	
Date	07/12/2013
Status	Final
Version	1.02

Related SP / WP	WP4	Document Reference	D44.2
Related Deliverable(s)	44.1, 22.x	Dissemination Level	PU
Lead Participant	EEMA	Lead Author	Jon Shamah
Contributors	Jon Shamah (EEMA); Charles Bastos Rodriguez (ATOS); Sebastian Kurowski (FHG) Monika Drabik (CA) Jens Kubieziel (AG)	Reviewers	Moritz Horsch (TUD) Meiko Jensen (ULD)

This document is issued within the frame and for the purpose of the FutureID project. This project has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under Grant Agreement no. 318424.

1. Executive Summary

This deliverable will provide the relevant requirements for a smooth integration of applications into the FutureID Infrastructure using the Application Integration Service (AIS). . It will focus on requirements that the AIS has to fulfill in order to allow integration of applications without causing complex adjustments for the application provider and will be a refinement of the general requirements identified in WP2.2.

This deliverable should be seen as a high level document providing design guidelines for the AIS rather than a definitive technical specification document

This deliverable is non-exclusively dependent on the outputs from:

- Task 22.1: Technical Requirements Analysis
- Task 22.2: Security Requirements Analysis
- Task 22.3: Privacy Requirements Analysis
- Task 22.4: Usability Requirements Analysis
- Task 22.5: Socio-Economic Requirements Analysis
- Task 22.6: Legal Requirements Analysis
- Task 22.7: Accessibility and e-Inclusion Requirements

We conclude that the AIS should enable interoperability with different EAI solutions and protocols, be easy to extend and to integrate for the service provider. Integration of the Application and should be usable and accessible. Additionally, the AIS should be secure, in order to enable trustworthy communication between the remaining FutureID infrastructure and the Application.

It is anticipated that there will be a further release of this deliverable as specifications evolve in other work packages.

2. Document Information

2.1 Contributors

Name	Partner
Jon Shamah (JS)	EEMA
Charles Bastos Rodriguez (CBR)	Atos
Nuria Ituarte Aranda (NI)	Atos
Sebastian Kurowski (SK)	FHG
Monika Drabik (MD)	CA
Jens Kubieziel (JK)	AG

2.2 History

Version	Date	Author	Changes
0.001	22/03/13	JS	Initial
0.002	29/03/13	CBR	Draft content
0.003/3a	07/06/13	SK	Draft content
0.004	11/06/13	JS	Draft content
0.005/6	27/06/13	JS	Draft content
0.007	02/07/13	JS	Section 7 reformatted
0.0071	10/07/13	SK	Section 6.4 added Retitled 6.1
0.0081	10/07/13	JS	Section 7 enhanced
0.009	15/07/13	JS	Section 8 added Appendix 1 added
0.010	17/07/13	MD	Draft of section 6.3 Draft of section 6.8 Section 7 enhanced
0.011	22/07/13	JS	Requirments numbering rationalised
0.012	23/07/13	NI	Addition to Section 7.8
0.013	05/08/13	SK	Changes to Section 6 and 8
0.014	06/08/13	JS	Fig, acronyms added and tidy
0.015	07/08/13	MD	Input to sections 6.3, 6.8, 7
0.017	08/08/13	MD	Changes in sections 6.3, 6.8 and Appendix
0.018	10/08/13	JK	Technical section added
		JS	Internal Review copy
0.019	22/08/13	JS	Adjusted review copy
0.020	27/08/13	JS/SK	Corrections
0.022	30/08/13	JS/SK	Final for release
0.0991	03/09/13	JS/SK	Final for release – small corrections
1.00	03/09/13	JS	Released Deliverable
1.01	06/12/13	JS	Modified release- new ref architecture

2.3 Table of Figures and Tables

2.4 Table of Acronyms

FutureID	Shaping the Future of Electronic Identity
AC-C	Application Client Connector
AIS	Application Integration Service
APS	Authentication Protocol Specification
A-DaC	Application Data Connector
AP	Application Provider
B2B	Business to Business
B2E	Business to Enterprise
BS-C	AIS Broker Service Connector
CA	Certificate Authority
CI	AIS Claims Interpreter
CIP	Competitiveness and Innovation Framework Programme
CT	AIS Claims Transformer
CTDB	AIS Claims Transformation Database
CV-C	AIS Credential Verifier Connector
DG CONNECT	Directorate General for Communications Networks, Content and Technology
DG Enterprise	Directorate- General for Enterprise and Industry
DG MARKT	Directorate General for Internal Market and Services
DIGIT	Directorate- General for Informatics
DoW	Description of Work
EAI	Enterprise Application Integration

EC	European Commission
eID	Electronic Identity
EU	European Union
FS	Federation Service
HTTP	Hypertext Transport Protocol
HTML	Hypertext Markup Language
ICT PSP	ICT Policy Support Programme
ICT	Information and Communication Technologies
IdP	Identity Service Provider
IdM	Identity Management
IE	Internet Explorer
iOS	Operation System from Apple; Trademark
LSP	Large Scale Pilot
MAC	Macintosh
M1	Month 1, M4-Month 4, etc.
MS	Member States
OS	Operation System
PC	Personal Computer
PDA	Personal Digital Assistant
SAML	Security Assertion Markup Language
SP	Sub Project
SSL	Secure Socket Layer
SSO	Single Sign-On
TLS	Transport Layer Security

TR	Technical Requirements
WP	Work Package

2.5 Referenced Documents

[1] epSOS Consortium, „epSOS: Home“, 2013. [Online]. Verfügbar unter: http://www.epsos.eu/. [Zugegriffen: 18-Apr-2013].
[2] ATOS, „ATOS eLearning“, ATOS please provide.
[3] FutureID Consortium, „Privacy Requirements“, Deliverable (Draft) D22.3, 2013.
[4] FutureID Consortium, „Usability Requirements“, Deliverable (Draft) D22.4, 2013.
[5] FutureID Consortium, „Socio Economic Requirements“, Deliverable (Draft) D22.5, 2013.
[6] FutureID Consortium, „Legal Requirements“, Deliverable (Draft) D22.6, 2013.
[7] FutureID Consortium, „Technical Requirements“, Deliverable D22.1, Sep. 2013.
[8] FutureID Consortium, „Security Requirements“, Deliverable D22.2, Sep. 2013.
[9] FutureID Consortium, „Accessibility and Inclusion Requirements“, Deliverable D22.7, Sep. 2013.
[10] FutureID Consortium, „Decsription of enterprise application infrastructures and their requirements for integration“, Deliverable D44.1, 2013.
[11] S. Cantor, J. Kemp, R. Philpott, und E. Maler, *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0*. 2005.
[12] O. Foundation, *OpenID Authentication 2.0*. .
[13] FutureID Consortium, „D23.3 - Common Documentation Guidelines“, Deliverable D23.3, 2013.
[14] E. Sauerwein, F. Bailom, K. Matzler, und H. H. Hinterhuber, „The Kano model: How to delight your customers“, *International Working Seminar on Production Economics*, Bd. 1, S. 313–327, Feb. 1996.
[15] C. Berger, R. Blauth, D. Boger, C. Bolster, G. Burchill, W. DuMochel, und D. Walden, „Kano’s methods for understanding customer-defined quality“, *Center for Quality Management Journal*, Bd. 2, Nr. 4, S. 3–36, 1993.
[16] FutureID Consortium, „Requirements Report“, Deliverable D34.1, 2013.
[17] FIDIS Consortium, „D3.13 Study on Usability of IMS“, FIDIS, Sweden, Germany, Deliverable D3.13, 2009.
[18] E. M. Rogers, *Diffusion of Innovations*, 5. Aufl. New York: Free Press, 2003.
[19] European Commission, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. .
[20] S. Bradner, „Key words for use in RFCs to Indicate Requirement Levels“, IETF RFC 2119.

3. Table of Contents

4. Project Description

The FutureID project builds a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infrastructure for Europe, which integrates existing eID technology and trust infrastructures, emerging federated identity management services and modern credential technologies to provide a user-centric system for the trustworthy and accountable management of identity claims.

The FutureID infrastructure will provide great benefits to all stakeholders involved in the eID value chain. Users will benefit from the availability of a ubiquitously usable open source eID client that is capable of running on arbitrary desktop PCs, tablets and modern smart phones. FutureID will allow application and service providers to easily integrate their existing services with the FutureID infrastructure, providing them with the benefits from the strong security offered by eIDs without requiring them to make substantial investments.

This will enable service providers to offer this technology to users as an alternative to username/password based systems, providing them with a choice for a more trustworthy, usable and innovative technology. For existing and emerging trust service providers and card issuers FutureID will provide an integrative framework, which eases using their authentication and signature related products across Europe and beyond.

To demonstrate the applicability of the developed technologies and the feasibility of the overall approach FutureID will develop two pilot applications and is open for additional applications who want to use the innovative FutureID technology

Future ID is a three-year duration project funded by the European Commission Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318424

5. Introduction

The AIS should be seen as a single non-complicated interface with a minimum of internal complexity.

This deliverable collects the requirements from AIS specifications defined in WP22.x so that they may be matched with the various methods of integrating with the Application, whether the Applications utilise Enterprise Application Integration (EAI) Middleware or not.

In the cases the EAI solution is already deployed by the Service Provider, there may be constraints in the data flows between FutureID and the Service Provider to be considered.

Figure 1 indicates the scope of this deliverable in the case of an existing EAI deployment.

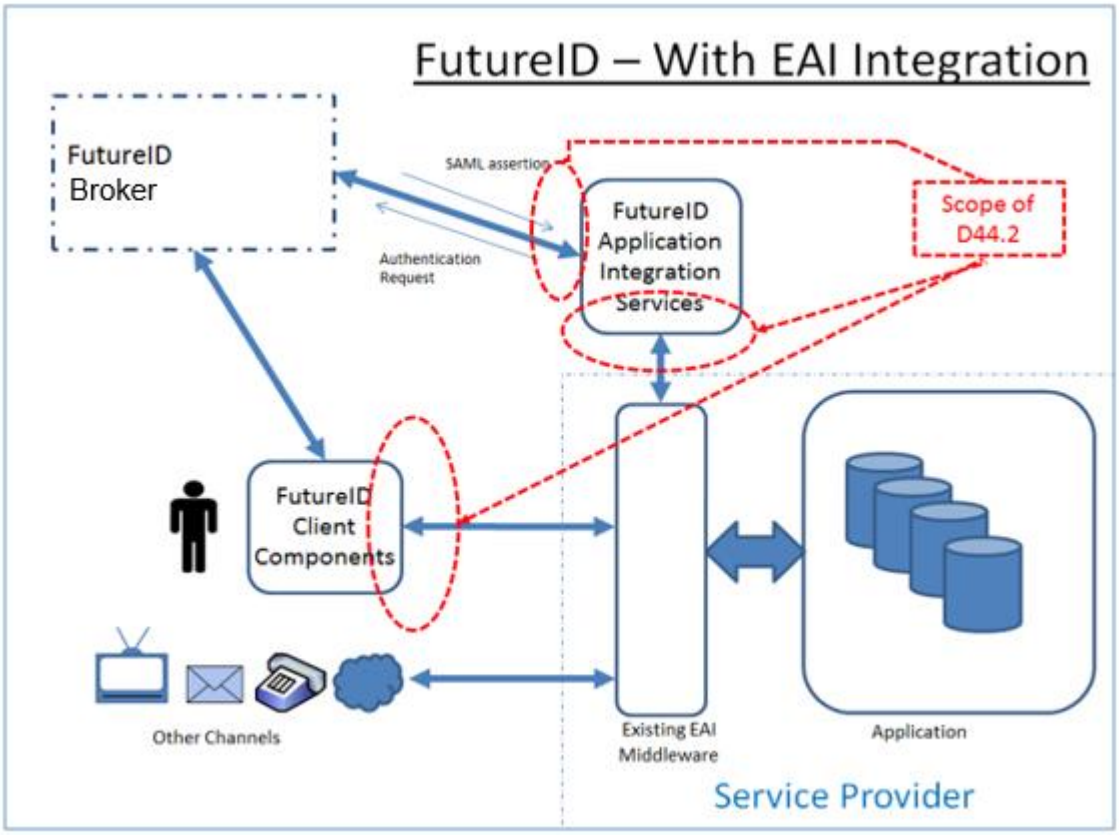

Figure 1: Scope with EAI

Figure 2 indicates the scope of this deliverable in the cases where a direct integration with applications is required:

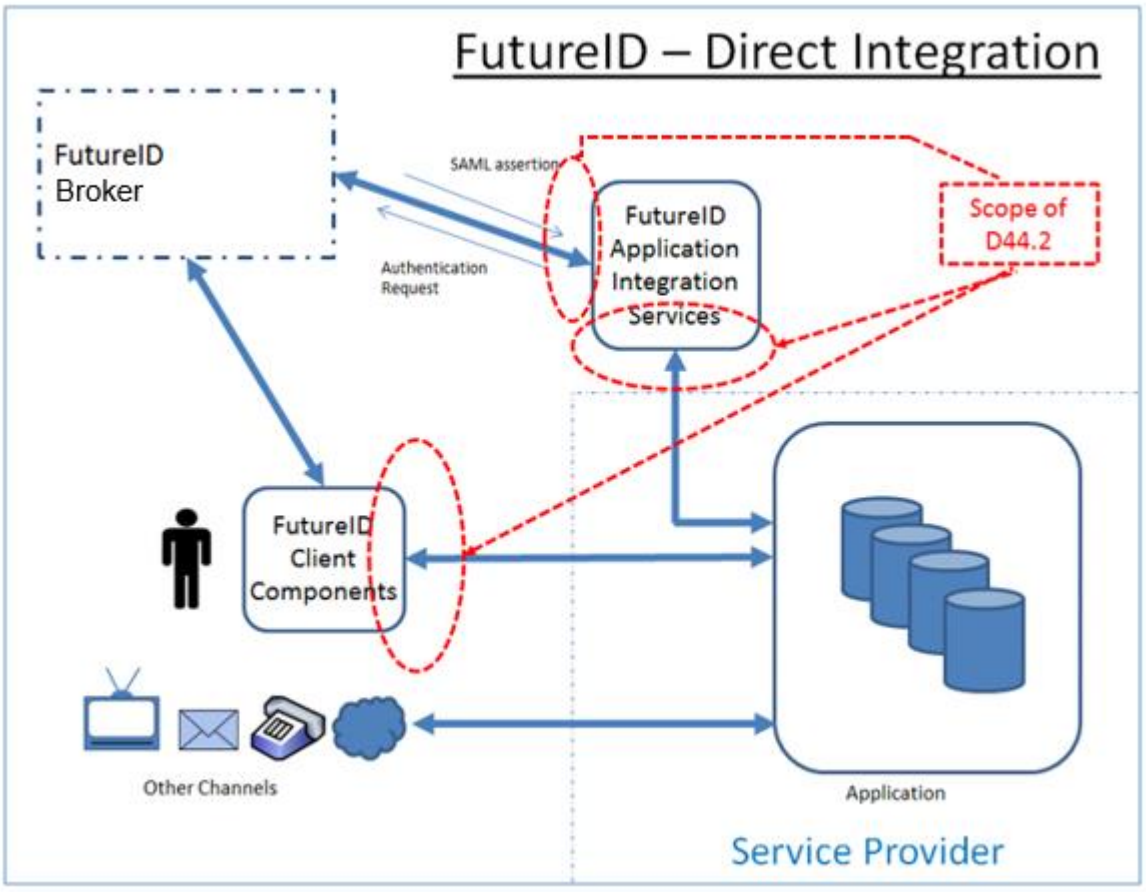

Figure 2 Direct Integration

The ability to easily link FutureID to Application is fundamental to ensure a wide take-up of FutureID services. The breadth of the FutureID features differentiates it from current federation solutions and so must be reflected in the communication.

It should be noted that both the initial FutureID pilots, ie European project epSOS [1] and Atos e-Learning Services for Enterprises [2] do not have EAIs deployed.

It is anticipated that there will be a further release of this deliverable as specifications evolve in other work packages.

6. Rationale of Domain Specific Requirements

6.1 Introduction and Typologies

Throughout D44.1 an abstract reference architecture was established for integrating the application and EAI. The following section lists the requirements as defined by deliverables D22.x and also considers D44.1 requirements for EAI integration.

At this state, the FutureID project holds resources for defining the socio-economic requirements to the AIS, by including the draft of the infrastructure requirements (D22.1-D22.7) [3]–[9] , as well as [10], which includes a first architecture, and analysis of possible use cases and existing EAI systems.

Additionally, an analysis is being conducted on use cases of EAI, in inter-organisational, and intra-organisational contexts. The analysis hereby concludes, on the following requirements of EAI in both contexts:

- Integration of Application and EAI IdPs

  As far as possible, identity providers from both, packaged applications and EAI systems should be included. However, this may only be possible within the boundaries of known standards, such as SAML [11] and by communicating with the client.

- Federation of Provisioning

  Support / Enabling the Triggering of Provisioning Processes

- Support of Industrial Trust Services

  Industrial Services may serve as Identity Providers, similar to OpenID [12] solving the issue of dissemination of identities for cloud applications. Also, such industrial Trust Services ease the issue of trust propagation for organisations.

- Integration of industrial IdPs

  Companies should be able to connect their IdP to the FutureID Broker Service, in order to be able to use the FutureID infrastructure, if required.

Repeating these findings, we are now able to derive the required typologies for the socio-economic requirements to the AIS. In the following we list, in accordance to D23.3 [13], the definitions of the stakeholders, priorities of the requirements to the stakeholders, a risk typology, and a requirements typology.

6.1.1 Stakeholders

- Application User

  The user of a service in the case of the AIS, would be the user of an application which is integrated into an EAI. Therefore we refer to the user as the application user. It is important to mention, that in the case of AIS we refer to users in a B2E, and B2B situation.

- Application

  The Service Provider in the case of the AIS, can be divided into two separate entities: An application and an EAI. Throughout [10] we referred to this division, while discussing potential authentication benefits resulting from using the FutureID infrastructure in both authentication at an EAI, and authentication while using an application (e.g. for data control). The Application uses the infrastructure for data control.

- EAI Service

  Integration Service Provider, in the case of using the AIS for authentication along with an EAI.

- Local Authentication Service

  The local authentication service includes any authentication, and identity provisioning mechanisms, which might be integrated in already existing EAI/applications, or organisations.

6.1.2 Stakeholder Priority

The priorities of the requirements are being assigned according to the KANO-Model [14], [15]:

- Exciter
  The requirement is not necessarily articulated, but may lead to excitement for the stakeholder. Addressing of the requirement is thus beneficial, but not necessary.

- Performance

The requirement is being explicitly wished for. Non-addressing of the requirement leads to dissatisfaction of the stakeholder.

- Basic

  The requirement is not articulated, but assumed to be integrated. Non-addressing of the requirement leads to dissatisfaction of the stakeholder.

As this document provides an overview on the domain specific requirements to the AIS, in order to consolidate these requirements, a prioritisation of the requirements will not be conducted. However, these levels might be useful for further analysis throughout later phases of the AIS development, if necessary.

6.1.3 Risk Types

[13] provides a first suggestion on different risks. Although these are defined as integrity levels in terms of testing documentation, requirements documentation at this state may benefit from these definitions. Therefore the levels are included in the definition of the requirements.

Description	Level
Software must execute correctly or grave consequences (leakage of person based data) will occur. No mitigation is possible.	4
Software must execute correctly or the intended use (mission) of system/software will not be realised causing serious consequences (leakage of linkable data). Partial-to-complete mitigation is possible.	3
Software must execute correctly or an intended function will not be realised causing minor consequences. Complete mitigation possible.	2
Software must execute correctly or intended function will not be realised causing negligible consequences. Mitigation not required.	1

As this document provides an overview on the domain specific requirements to the AIS, in order to consolidate these requirements, a risk assessment of the requirements will not be conducted. However, these levels might be useful for further analysis throughout later phases of the AIS development, if necessary.

6.1.4 Requirement Types

According to [10] the AIS will need to address different types of requirements. At this state, it makes sense to distinguish between functional and non-functional requirements. Throughout the different disciplines, this typology can be further refined (Section 6.4-6.8).

- Functional Requirements
  - Technical Functions

- Non-functional
  - Security / Trust
  - Privacy
  - Adoption & Acceptance
  - Usability
  - Legal
  - Accessibility & Inclusion

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [16].

6.2 Technical

The purpose of this section is a definition of the technical requirements of the AIS. The deliverable D44.1 [10] includes a survey about current EAI platforms. Beginning with the abstract architecture in chapter 9 we started to derive technical requirements. The main purpose of the AIS is communicating with several parts of the FutureID and company infrastructure. So it is important that the AIS supports a large variety of protocols. For easy extension of future protocols and standards it seems important that the AIS uses an extension or plugin architecture.

It is important to mention, that the point-of-view of these requirements on the AIS is from a pure technical perspective. Therefore logging mechanisms are not necessarily regarded, e.g. under a legal or privacy perspective. For instance, requirement TE-06-01 includes an adjustable logging mechanism, which should offer the possibility for the service provider to adjust the level and types of stored data, according to the circumstances of the AIS usage.

6.3 Security

This section defines the security requirements of the FutureID AIS, and it has been written in accordance with the draft of D22.2-Security Requirements analysis [8]. Since AIS allow the

communication between the appropriate FS – as a part of FutureID Infrastructure - and the Application – as a part of Service Provider -, they are relevant components of FutureID architecture and ensuring their security is a really key issue.

The security can be defined by four characteristics: confidentiality, integrity, availability and accountability. All of them should be provided not only for the normal operation of AIS, but also in the case of an accident.

Issues relating to the security requirements for AIS can be divided into several thematic groups, such as: identification and authentication, data protection, trusted channel, cryptographic support, security management, access control.

As the AIS may be required to process information from the Application and the remaining FutureID infrastructure, the technical requirements also include requirements to processing issues, e.g. ensuring data integrity during processing information transmitted by the federation service (FS) (see SE-02).

6.4 Privacy

Deliverable D22.3 [3] lists privacy protection goals and derives requirements among these protection goals. The privacy protection goals are being defined as unlinkability, transparency, and intervenability. Unlinkability means “that privacy-relevant data cannot be linked across privacy domains or used for a different purpose than originally intended” [3]. This does include, that information of the subject is being held, and processed apart from the information regarding the identity, or the identities characteristics. It also implies a minimisation of data to be processed. Transparency is defined as ensuring “that all privacy-relevant data processing including the legal, technical and organisational setting can be understood and reconstructed.” [3]. This means that an understanding must be provided on both the planned processing (defined as ex-post transparency), and “the time after the processing has taken place” [3] (defined as ex-ante transparency). Intervenability is being defined as ensuring “that data subjects, operators and supervisory authorities can intervene in all privacy-relevant data processing.” [3]. Conclusively these privacy protection goals lead in [3] to requirements, regarding the privacy protection goals of linkability and transparency, demanding the minimisation of personal data, the limitation of linkability of personal data, knowing about the processing lifecycle for all pieces of personal data, general, and context-specific information of the users, the support of transparency requests, and the audit logs. Intervenability is being addressed as supporting user interaction, correction and erasure requests, and establishing a helpdesk.

While the minimisation of personal data (PR-01), the limitation of linkability of personal data (PR-02), knowledge about the processing lifecycle (PR-03), general and context-specific informing of the user (PR-04), support of transparency requests (PR-05) and user interaction (PR-06), and

correction (PR-07) and erasure requests (PR-08), can be addressed by the AIS, the authors argue that the establishment of a helpdesk and creation of audit logs may be out of scope of the AIS, since it may provide only a module able of processing authentication processes, neither including authorisation, nor any other processing and handling of personal data. It therefore may be integrated as part of an EAI, for which the establishment of a helpdesk, and the creation of audit logs are reasonable.

6.5 Usability

In their current state, the Usability requirements in Deliverable D22.4 [4] build upon general requirements to usability and refines them towards their usage in user interfaces. Since the AIS does not include a user interface, the requirements in D22.4 [4] are not completely applicable to D44.2. However, some requirements are still relevant for the AIS, and are thus listed in the requirements breakdown.

The stakeholder being addressed is the Application User. The Application User is hereby being interpreted as a job-related user, as defined in D34.1 [16]. The motivation to use FutureID for this user is hereby stated as “She could save a lot of time, if she wouldn’t need to type in her password every time. Also for many different work related applications, she would benefit from a central system able to provide the needed functionality.“ [16].

The Application User hereby brings basic knowledge on security updates and password protection, and owns multiple credentials. By further analysis the requirements in [16] identified issues for the Application User, when using FutureID. The analysis distinguishes between system tasks and interaction tasks, whereas system tasks refer to the ability. The following shows the interaction and system tasks, which are problematic for the Application User. Problematic system tasks require further explanation, in order to enable understanding of the system tasks by the Application User. Interaction tasks, require further assistance, since problems with functions yield a misusage of the software.

The following lists provides an overview on the ease-of-understanding / ease-of-use of the interaction and system tasks, given the application user is a job-related user, as defined in D34.1 [16].

1. System tasks
    a. Show credential attributes
    b. Grant access to credential store
    c. Provide information on current authentication status, upcoming events, and required information
    d. Show required attributes for service (affirmations/declarations)

   e. Show status of anonymity
   f. Indicate threat of compromising anonymity per attribute
   g. Show error message
2. Interaction tasks
   a. Manage credentials
   b. Select authentication credential
   c. Store credentials on mobile device or smart card
   d. Establish link between credentials and attributes
   e. Display certificate (to others), graphically present credential (Barcode)
   f. Transmit credentials (to verification device, for others)
   g. Verify License / credentials (to others)
   h. Gain access control to credential store
   i. Bind credential to device
   j. Chose way of authentication from multiple options
   k. Use different platforms/means of authentication/identification
   l. Sign a document or contract
   m. Encrypt/Decrypt a document

[16]

Many of these tasks refer to the user interface. Yet the AIS is in some cases required to provide information in order to enable the user interface to provide additional assistance / explanation. This refers to 1.d, 1.e, 1.f, 1.g, and 1.h. Therefore the AIS requirements breakdown mainly contains requirements to provide information for explaining these system tasks.

D22.4 further quotes a study on the usability of Identity Management Systems [17], which are broken down into 5 properties:

1. Unmotivated user property:
   Security is not the main task.
   The user is unlikely to invest a lot of time and effort.

2. Lack of feedback property:
   The user needs precise feedback to make well-informed decisions, but security configurations tend to be complex and are difficult to communicate to the user efficiently.

3. Abstraction property
   Security concepts often use sets of abstract rules. That makes them hard to understand for laypeople.

4. Barn door property

Once committed, a security critical user error cannot be undone. Once unprotected, a secret is gone.

5. Weakest link property
   The security of a system is only as strong as its weakest link. So the user must be guided through all relevant parts of his security configuration.

Here, especially the Weakest Link property may yield further requirements to the AIS, indicating further requirements for informational support of the user by the AIS. Therefore the following requirements breakdown addresses these issues by informing about the authentication and its consequences (US-01), showing attributes required by the Application or EAI (US-02), providing information on the status of anonymity (US-03), and providing error messages (US-04). The indication of threats of compromising anonymity per attribute, as described in D34.1 [16], will not be included, since the authors believe, that such an indication requires knowledge, which should be held by the client infrastructure. It will however be supported by providing information on the required attributes for a service (US-02) and information on the status of anonymity (US-03).

6.6 Socio-Economic Requirements

The Socio-Economic perspective on the requirements enables a design of the application integration service, while aligning to market expectations. This aids in adoption of the AIS, by maximising its utility due to stakeholder alignment.

The socio economic requirements introduce additional non-functional requirements. In order to be able to categorise these requirements, we extend the non-functional requirements:

- Non-functional
  - Trust
  - Security
  - Privacy
  - Adoption
    - Service provider adoption
    - Perceived Utility
  - Usability
  - Legal
  - Accessibility & Inclusion

Using this typology, the following lists the aspects of socio-economic requirements, which are being distilled from [10] and [5].

Service Adoption

[5] provides at its current state an insight into the socio-economic view on FutureID. Using these findings, we learn, that the acceptance / adoption of the FutureID infrastructure is subject to a two-sided market. Therefore „if more users adopt a SSO system, more services will adopt, and the other way around" [5]. In the terms of the AIS this would imply, that both the user adoption, and the service adoption should be addressed, e.g. by implementation of interfaces to as many EAI infrastructures as possible, or by supporting the most common protocols. The requirement of service adoption is being addressed in requirement item SC-01.

User Adoption

On the side of the user adoption, we argue, that this may be part of usability and utility. We argue, that usability may be subject to the FutureID Client, and is thus included in Subproject 3 of the FutureID project. However, utility, in terms of perceived utility largely influences the adoption of the AIS. In [5] we learn, that "It has been argued that insecurity and trust issues can make IMS fail, which was one of the motivators for the privacy-enhancing IdM movement" [5], implying that the utility of the AIS might be subject to matters of trust. Yet, according to the findings in [5], this may not necessarily lead to technical implementations, since "It has been argued that insecurity and trust issues can make IMS fail, which was one of the motivators for the privacy-enhancing IdM movement" [5]. Yet, the requirements to trust is being addressed in requirement item SC-02.

We also learned, that utility may be positively influenced by reduced sign-on (SC-03), privacy (SC-04), reduction of user-interaction (SC-05), identity intermediation (SC-06), and security (SC-07). While, the liability (SC-08) of the IdP, and occurring usage, and implementation costs (SC-09) may negatively influence the perceived utility.

From [18], we additionally learn, that this perceived utility, is also subject to the perceived advantage over the existing alternatives. Therefore all requirements (SC-02 to SC-09) on the mentioned issues are being articulated relatively to existing alternatives.

As issues, such as privacy issues, reduction of user interaction, and intermediation are handled by the remaining FutureID infrastructure (e.g. the Broker Service), the requirements SC-04, SC-05, and SC-06 are not mission critical for the AIS. However, as D44.1 showed that the AIS may require additional functionalities of processing the authentication data, e.g. in order to enable a secure frontend, or authentication of the information exchanged by the Application, these requirements are included in the requirements to the AIS.

6.7 Legal

As part of the FutureID infrastructure, the AIS is an element, which enables authentication to the Application, and EAIs (see D44.1 [10]). As such, it is part of the FutureID infrastructure, which processes identity data, and thus personal data according to Directive 95/46/EC [19]. Yet, while

e.g. the Broker Service may be subject to an additional layer in front of filing systems, creating a filing system itself, the AIS simply forwards information to the Application / EAI, neither storing it, nor organising any mediation between storages. The Directive 95/46/EC however, only applies to filing systems, defining filing systems as “any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis” [19]. Since the AIS does not necessarily include any “structured set of personal data” in terms of storing the data, but simply forwards this data after processing, the directive may not apply to the AIS, if requirement SC-01 is being fulfilled.

Beyond the considerations and requirements outlined here, the FutureID AIS must also comply with the requirements stated in D22.6

6.8 Accessibility and e-Inclusion

The e-Inclusion is a social movement whose goal is to end the digital divide of people, that have and don’t have capabilities and acces to use Information Technology. As the AIS is a backend component, aiming at integrating the Application in the FutureID infrastructure, Accessibility and e-Inclusion could be understood as the aspiration to let different service providers integrate with the FutureID infrastructure. While these requirements are important for the infrastructure as a whole, the underlying definition bends the term of e-Inclusion towards a business perspective of integration and usability. Therefore these issues have been adressed as usability requirements to the AIS in US-05 to US-14.

Beyond the considerations and requirements outlined here, the FutureID AIS must also comply with the requirements stated in D22.7 [9].

7. Summary of Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [20].

7.1 Technical Requirements for AIS

No	TE-01
Description	The AIS SHOULD support a great variety of protocols. The AIS component has to communicate with different kind of software. The protocol support of those software has a very small subset. So AIS has to support a wide range to be successful.

No	TE-01-01
Description	The AIS MUST support SAML. In D44.1 it is stated that all current EAI systems use at least SAML. So SAML seems to be the least common multiple. SAML is essential.

No	TE-01-02
Description	The AIS MUST support SOAP. Almost all of the EAI middleware systems make use of SOAP. It is a necessity for successful integration to have SOAP support.

No	TE-01-03
Description	The AIS SHOULD support WS-* standards. D44.1 suggests that the EAI-CV-C interface will be realised as web service.

No	TE-02
Description	The AIS MAY support multiple existing protocols. In D44.1 it was stated that EAI systems make use of different protocols. The initial AIS may support them from start.

No	TE-03
Description	The AIS SHOULD be easily extendible via a plugin or extension concept. This enables the use of other components and helps to include new protocols in the future.

No	TE-04
Description	The Claims Transactions Database (CTDB) MUST be conform to the SQL standard (at least SQL:2003 or any newer version). This ensures that different SQL-based databases can be used.

No	TE-05
Description	The CTDB MAY support NoSQL databases. Companies use sometimes non-relational databases, esp. NoSQL. So it might be useful to also support them in the CTDB.

No	TE-06
Description	The AIS MUST support logging of different events. The logging is needed to find errors and misconfigurations.

No	TE-06-01
Description	The AIS SHOULD support different levels of logging. The log levels should range from no logging at all to a very detailed level (for debugging purposes).

7.2 Security Requirements for AIS

No	SE-01
Description	The requests to the BS/FS SHOULD be signed by the application using a certificate issued by an authorised Certificate Authority.

No	SE-02
Description	Resolving of the information from the FS MUST be possible only once. The second request to resolve the artifact should return only the boolean information if the artifact is already resolved.

No	SE-03
Description	The request for resolving the artifact MAY be encrypted using the server public key.

No	SE-04
Description	Cookies created by the AIS MUST be created on the concrete domain with the option HttpOnly

No	SE-05
Description	The AIS MUST require a re-authentication with AS and FS of a user in case of following events: session inactivity of more than 5 minutes, loss of connectivity to FutureID server, device authentication error, data integrity error (e.g.integrity error transmiting eID data) and failure in establishing a trusted channel

No	SE-06

Description	In case that the AIS, the Application or the FS detect a data integrity error, the AIS MUST close the session and wait for a re-authentication of the user.

No	SE-07
Description	The AIS MUST ensure that any security or privacy relevant data from a previous session is deleted and made unavailable as soon as the session is closed or the communication is interrupted.

No	SE-08
Description	The AIS MUST reject connections with unsuccessful authentication

No	SE-09
Description	The AIS MUST perform the following actions upon detection of a potential security violation: session termination, residual data deletion, key destruction and security attribute expiration.

No	SE-10
Description	Tokens created by the AIS SHOULD be encrypted with an application key

No	SE-11
Description	Tokens created by the AIS MAY be signed with the AIS private key with a certificate, that is trusted by the SP

No	SE-12
Description	Tokens created by the AIS MUST have validity time

No	SE-13
Description	Validity time of the authorisation tokens MUST be verified at each request to the SP

No	SE-14
Description	Tokens created by the AIS MUST contain attributes only to the concrete SP

No	SE-15
Description	The AIS MUST avoid the storage of any security relevant data, like authentication data and eID data, if possible

No	SE-15-1
Description	If the storage of security relevant data (as in SE-15) is necessary, the AIS MUST ensure that those security relevant data as well as the log files are protected

No	SE-15-2
Description	Stored security relevant data (as in SE-15) MUST NOT be modified or deleted.

No	SE-15-3
Description	The AIS must ensure the integrity of data sent to the FS

No	SE-16
Description	The AIS MUST avoid unnecessary access

No	SE-16-1
Description	The AIS MUST restrict a limit of one session per user at the same time

7.3 Privacy Requirements for AIS

No	PR-01
Description	The AIS SHALL require and demand as less personal data as possible during the authentication process

No	PR-02
Description	The AIS SHALL not process personal data in one process step and apart from other required data of the authentication

No	PR-03
Description	The processing of the AIS, as well as included responsibilities and, processed information SHOULD be documented clear and understandable

No	PR-04
Description	The AIS SHALL provide information on the current authentication, the authentication process, and any information processed to the client

No	PR-05
Description	The AIS SHALL provide the possibility to disclose any information of a subject upon the request of the subject corresponding to the information.

No	PR-06
Description	The AIS SHALL provide the possibility to interact with any information processing during the authentication to the subject.

No	PR-07
Description	The AIS SHALL provide the possibility to alter and halt any information processing during authentication to the subject

No	PR-08
Description	The AIS SHALL provide the possibility to reverse any information processing and to delete processed information during authentication to the subject

7.4 Usability Requirements for AIS

No	US-01
Description	The AIS SHALL provide information on the current authentication status and upcoming authentication events to the client

No	US-02

Description	The AIS SHALL provide information on required data of the current authentication status and upcoming authentication events to the client

No	US-03
Description	The AIS SHALL provide information of the type of required data of each authentication step to the client

No	US-04
Description	The AIS SHALL provide error messages occurring throughout authentication to the client

No	US-05
Description	The AIS SHOULD be as easy as possible to install to let different service providers integrate with FutureID

No	US-06
Description	The AIS SHOULD have a well prepared installation documentation, that delivers also information about sustainability

No	US-07
Description	The AIS documentation SHOULD be translated into different languages

No	US-08
Description	The AIS components SHOULD be able to use on different platforms

No	US-09
Description	The AIS components SHOULD be sustainable

No	US-10
Description	The AIS components MAY have a standardised method of reporting its‘ current status and should suggest possible workarounds and solutions to problems

No	US-11
Description	Messages [warnings/errors] SHOULD be provided in a clear and understandable form not using closed security ontology

No	US-12
Description	An installation and configuration assistant MAY be provided

No	US-13
Description	The AIS MAY be equipped with an automatic self-test feature for early detection of potential instabilities and other issues

No	US-14
Description	The AIS components MUST provide a high level of confidentiality through the use of appropriate authentication methods

7.5 Socio-Economic Requirements for AIS

No	SC-01
Description	The AIS SHALL enable an easy integration of existing Application and EAI infrastructures

No	SC-02
Description	The AIS SHALL increase trust over preexisting authentication mechanisms

No	SC-03
Description	The AIS SHALL reduce required sign-on mechanisms for the user

No	SC-04
Description	The AIS SHOULD address privacy issues during authentication and data control

No	SC-05
Description	The AIS SHALL reduce the required user interaction with regard to existing authentication mechanisms for EAI.

No	SC-06
Description	The AIS SHALL intermediate between existing eIDs

No	SC-07
Description	The AIS SHALL provide sufficient security features for handling corporate information.

No	SC-08
Description	The AIS SHALL avoid liability of the user in the case of occurring damage

No	SC-09
Description	Implementation and usage of the AIS SHALL be cheaper than other authentication and data control mechanisms.

7.6 Legal Requirements for AIS

No	LE-01
Description	The AIS SHALL NOT store any personal data processed during authentication

No	LE-02
Description	The AIS SHALL use and transmit the user credentials and sensitive data securely

No	LE-03
Description	The AIS MUST keep the integrity of the data. The data must keep the integrity and if some data need to be translated, this must be carried out in accordance with the translation specifications (see OT-01).

No	LE-04

Description	The AIS MUST only request the neccesary attributes from the user for performing the accordant task.

No	LE-05
Description	The AIS MUST comply with the legal requirements originating from the legal considerations performed in D22.6 [6]

7.7 Other Requirements for AIS

No	OT-01
Description	The AIS MUST have a Protocols translation specifications that maps the data from Service Provider to a message (a SAML assertion) for the FS.

8. Definition Conflicts and Resolutions

The following provides an overview on possible conflicts between the requirements. In order to enable better understanding of the origin of conflicts, we use the abstract architecture developed throughout D44.1 [10].

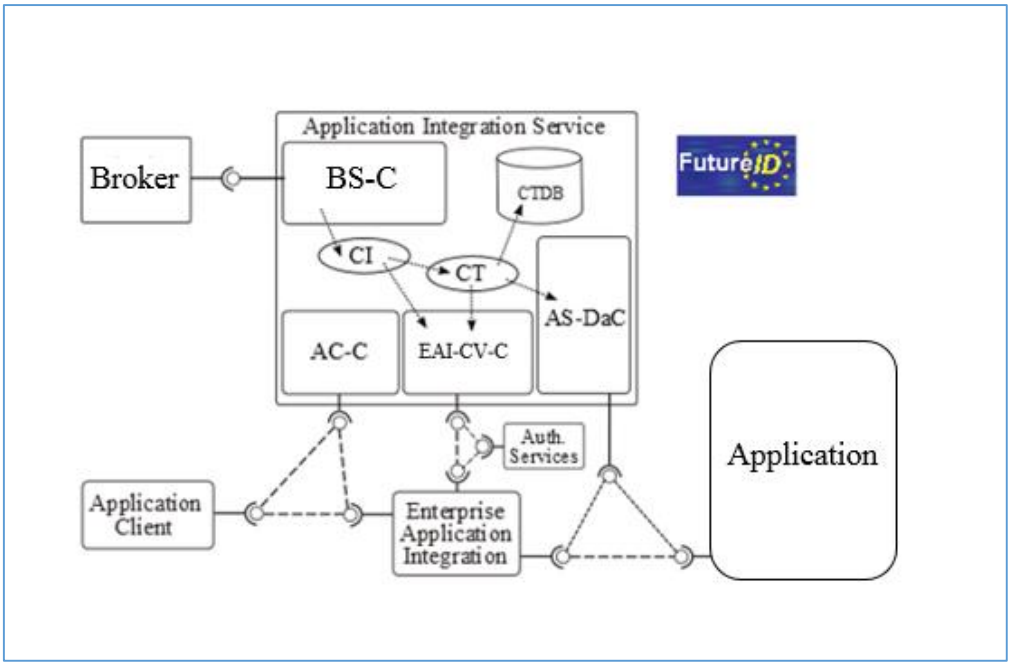

Figure 3 Abstract architecture of the application integration service [D44.1]

Figure 3 shows the application integration service (AIS) and its modules. These comprise of the Broker Service Connector (BS-C), the Application Client Connector (AC-C), the EAI Identity and Credential Verifier Connector (EAI-CV-C), and the Application Data Connector (A-DaC), and the Claims Transaction Database (CTDB). The following provides a short overview on these components:

- Broker Service (BS)
  - The BS-C connects both to the A-DaC and the EAI-CV-C, forwarding necessary authentication data to the EAI-CV-C for initial authentication when launching an Application, or accessing an EAI, and to the A-DaC for authenticating information flows, leaving the Application (if necessary). The BS thus enables communication of the EAI and the Application with the Broker Service and vice-versa, both in Claims Interpreter (CI) and Claims Transformer (CT) mode.

- Application Client Connector (AC-C)
    - The application client connector enables interaction of the AIS with the application client. As some applications may include a multi-layer architecture with an external client (e.g. web-based), the AC-C allows to introduce any further interaction with the client (if necessary).
- EAI Identity and Credential Verifier Connector (EAI-CV-C)
    - The EAI-CV-C is the central component for initial authentication of a user at an EAI or applications service. It passes the authentication data, as received by the BS, forward to the EAI or Application, and forwards the response of the EAI or Application to the BS for further processing.
- Application Data Connector (A-DaC)
    - In the abstract architecture of the AIS, as in [10] the A-DaC was introduced in order to enable authentication of the data flow of an application. [10] states, that "in many cases, the Application may need additional verification of certain information contained within the service request. For instance, if the particular Application must be tailored to a specific user identity, it becomes necessary to deliver that information from a trustworthy source towards the Application implementation." [10]. The A-DaC therefore handles additional authentication of information access done throughout the information flows of the Application, which makes it subject to issues of security, privacy, and legal requirements.
- Claims Transaction Database (CTDB)
    - The CTDB is a stand-alone database, which allows for investigating errors, which may occur throughout the authentication. It therefore serves as a logging module for the AIS.

This architecture provides an early insight on the components, and thus possible information flows. By mapping the requirements of Section 7 to architecture, we are able to isolate possible conflicts in the architecture. The following provides an overview on possible conflicts. The mapping of the requirements can be found in Appendix 1.

8.1 Requirements Conflicts During Logging of the Authentication Process

Since the CTDB shall log the authentication process and the authentication information, this violates requirement LE-01-01. This conflict occurs, when personal data is stored among the logged authentication process. However, TE-06-01 allows for adjusting the details of the logging

process. This may help in deciding, which information is really required, and thus meet the requirement of minimisation of required information, as in PR-01-01.

8.2 Requirements Conflicts During Processing of the Authentication Information

Conflicts occurring during processing of the authentication information occur in the security, privacy and socio-economic requirements. The following Table 1 provides an overview on the conflicting requirements.

Requirement	Conflicting Requirement	Description of conflict
SE-01, SE-03, SE-09	SC-01	The inclusion of certificates and Public Key Infrastructures yields costs. The requirement thus may conflict the easy integration of The Application, if these mechanisms create too high costs for the Service Provider.
PR-03	SC-01	As the inclusion of the AIS into the Service Providers processes may not allow for a standardised documentation, this may create additional work, and thus higher costs for the Service Provider.
PR-08	SC-03, SC-05	While halting the information processing during authentication, the deletion of authentication data submitted to the Application may increase costs for the Service Provider, since additional mechanisms may be required.
LE-01	All functional requirements	The AIS may be required to store data, at least for limited time. Depending on the legal interpretation of “storing data” this requirement may not be fully addressable. For instance, even if information is only forwarded by the AIS component, information is

		stored in the main buffer, requiring the AIS to comply to the legal framework of the European data protection directive.

Table 1 Conflicts during processing of the authentication information

From a security perspective, signatures and certificates are required in order to increase trust of the application provider. While implementation of such trustworthy mechanisms allow for trust propagation and may thus increase adoption by the service provider, the existing costs may hinder service providers to include FutureID as an authentication method (SE-01-01, SE-01-03, and SE-01-09).

Privacy requirements, for documentation of responsibilities and the implementation of the AIS in an organisation, may yield additional workload for the Service Provider, creating additional costs and hinder the adoption. On the other hand, not-documenting violates the privacy goal of transparency, and leaves responsibility unclear to the user, a structured approach of documenting may be provided, during installation, in order to include this requirement.

Another conflict occurs with the deletion of information. As the AIS processes and forwards authentication information to the Application / EAI, this requirement can technically be fully addressed, during the authentication itself. Yet, after authentication, deletion of transmitted information at the Service Provider is not easy to integrate. As this may require additional mechanisms, and additional trust from the Service Provider, it increases implementation costs for the AP, and thus violates SC-01-01.

8.3 Resolutions of Conflicts

8.3.1 Inclusion of certificates and Public Key Infrastructures

Certificates may be included by a trustworthy Certificate Authority (CA), at the IdB. By centralising the certificate at the FutureID middleware, the security features of implementing certificates can be used, while decreasing costs for the Application. On the other hand this would only allow for proving the identity of the Broker Service and not include the authentication of the Application Provider towards the Broker Service, and thus towards the FutureID client. This raises a question of how to cost-effectively certify the identity of the Service Provider. As certificates are often included in the provided services, this question may not necessarily arise for every Service Provider. However, if certificates are not included in provided services, their inclusion should take into account the economic perspective as well, in order to avoid too high costs for the Service Provider, which may hinder the adoption of the AIS.

8.3.2 Documentation of responsibilities

The documentation of responsibilities yields additional costs for the Service Provider. However these costs can be lowered by offering an automated and structured approach for documenting processes and responsibilities. Such tools could be part of the assisted configuration and installation routines, as required by AC-01-08.

9. Conclusion on the Requirements and Paradigms for Implementation of the AIS

This document provides a breakdown and discussion of requirements for the AIS of FutureID. Throughout Section 6, we provided an overview on possible requirements from different perspectives, which were consolidated and checked for possible conflicts in Section 7 and 8. These requirements will provide directions for the technical specification and implementation, which is foreseen in the upcoming Deliverables D44.3, and D44.4.

It is possible, when consolidating the requirements to extract the following paradigms:

- Interoperability with protocols and different EAI solutions

  The AIS should offer interoperability of different protocols and enable the integration of different EAI solutions and applications. Mandatory protocols and technologies are listed in TE-01, TE-02, and TE-03.

- Extendibility and Integration

  The AIS must be easily extendible to the users' business needs. Additionally it should easily integrate into the users' business environment. Additionally the AIS should support an easy integration of applications and EAI, without further technical expertise. Additionally integration of the AIS into the users' business environment should be as cheap as possible.

- Documentation and Transparency

  The AIS should be fully documented, in order to enable extendibility and easy integration of the component into the business environment of the user. Additionally all responsibilities and roles, as well as the amount of data required, should not only be minimal, but also be adjustable and documentable.

- Usability and Accessibility

  The AIS should support the usability requirements of the FutureID Client, and aid during integration of applications and EAIs. Additionally the AIS should be able to provide the user with information on the amount and type of data being processed.

- Security

The AIS should provide sufficient security data to handle corporate information and enable a secure handling of the authentication information. It therefore should include sufficient security features.

1. Appendix: Requirements Rationale

1.1 Mapping of the Requirements to the Abstract AIS Architecture

Requirement	BS-C	AC-C	EAI-CV-C	AS-DaC	CTDB
Technical Requirements					
TE-01	■	■	■	■	
TE-01-01	■		■	■	
TE-01-02	■	■	■	■	
TE-01-03		■	■	■	
TE-02			■	■	
TE-03	■	■	■	■	■
TE-04					■
TE-05					■
TE-06	■	■	■	■	■
TE-06-01	■	■	■	■	■
TE-07	■	■	■	■	■
TE-08	■	■	■	■	■
TE-09	■	■	■	■	■
Security Requirements					
SE-01	■		■	■	
SE-02	■				
SE-03			■	■	
SE-04		■			
SE-05	■	■	■	■	
SE-06		■	■	■	
SE-07	■	■	■	■	
SE-08	■	■	■	■	
SE-09		■	■	■	
Privacy Requirements					
PR-01		■	■	■	■
PR-02	■		■	■	
PR-03	■	■	■	■	■
PR-04	■		■	■	
PR-05					■
PR-06	■		■	■	
PR-07	■		■	■	
PR-08	■		■	■	■
Usability Requirements					
US-01	■		■	■	
US-02	■		■	■	
US-03	■		■	■	
US-04	■		■	■	
US-05		■	■	■	
US-06	■	■	■	■	■
US-07	■	■	■	■	■
US-08	■	■	■	■	■
US-09	■	■	■	■	■
US-10	■	■	■	■	■
US-11	■	■	■	■	
US-12	■	■	■	■	■
US-13	■	■	■	■	
US-14	■	■	■	■	
Socio-Economic Requirements					
SC-01		■	■	■	
SC-02	■	■	■	■	
SC-03	■	■	■	■	
SC-04	■		■	■	■
SC-05	■		■	■	
SC-06	■		■	■	
SC-07	■	■	■	■	■
SC-08	■		■	■	
SC-09		■	■	■	
Legal Requirements					
LE-01	■	■	■	■	■
LE-02	■	■	■	■	
LE-03	■		■	■	
LE-04	■		■	■	
Other Requirements					
OT-01	■				