D22.1 – Technical Requirements Analysis

Document Identification	
Date	30/10/2013
Status	Final
Version	1.00

Related SP / WP	SP 2 / WP 22	**Document Reference**	Insert Reference #
Related Deliverable(s)	D21.1, D22.2, D22.3, D22.4, D22.5, D22.6, D22.7, D31.1, D31.2, D32.1, D32.2, D33.1, D34.1, D35.1, D36.1, D37.1, D44.2	**Dissemination Level**	CO
Lead Participant	IFAG	**Lead Author**	Detlef Houdeau (IFAG)
Contributors	G&D, IFAG, ATOS, CA, USTUTT, TUD	**Reviewers**	Roger Dean – EEMA Jon Shamah – EJC Thomas Gross – UNEW

Not to be distributed outside the FutureID Consortium

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

This document and its content are the property of the FutureID Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or

its contents are not to be used or treated in any manner inconsistent with the rights or interests of the FutureID Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the FutureID Partners.

Each FutureID Partner may use this document in conformity with the FutureID Consortium Grant Agreement provisions

Abstract

D22.1 conducts the technical requirements analysis based on D21.2 (technical inventory). A focus of this report is on the analysis of mandatory and optional functionality as well as existing interfaces of components in eID solutions that may or will set a technical standard for upcoming eID solutions.

D22.1 would be the basis of the FutureID reference architecture, which would be collected in D44.2. D22.1 is one pillar in a range of requirement analysis with:

- **Technical** requirements, D22.1 (present paper)
- **Security** requirements, D22.2
- **Privacy** requirements, D22.3
- **Usability** requirements, D22.4
- **Socio economic** requirements, D22.5
- **Legal** requirements, D22.6
- **Accessibility** and **inclusion** requirements, D22.7

With the specific focus on technical aspects D22.1 captures

- Technical requirements on services, mandatory
- Technical requirements on services, optional
- Technical requirements on platform (Client, Browser, Server)

The technical requirements must capture all relevant aspects of SP3, particularly with D31.1, D31.2, D32.1, D32.2, D33.1, D35.1 and D36.1.

Document Information

Contributors

Name	Partner
Detlef Houdeau	IFAG
Frank Michael Kamm	G&D
Nuria Ituarte Aranda	ATOS
Tomasz Grabowski	CA
Eray Özmü	USTUTT
Christoph Busold	TUD

History

Version	Date	Author	Changes
0.1	27/03/2013	Detlef Houdeau	Document Structure
0.11	05/04/2013	Detlef Houdeau, Simon Hartmann	Work share
0.12	26/07/2013	Detlef Houdeau, Simon Hartmann	Overworked Document Structure; Decision of the work share
0.13	31/07/2013	Eray Özmü	Copied the descriptions of the components from D22.2 and added Introduction (chapter 1.2)
0.14	02/08/2013	Detlef Houdeau, Simon Hartmann, Christoph Busold, Frank Michael Kamm	Table of content overworked; Chapter 4.2 completed Chapter 4.3 completed; Table of acronyms started;
0.15	05/08/2013	Detlef Houdeau, Simon Hartmann	Chapter 1, 2.1, 2.3, 3.1 and 3.3
0.16	08/08/2013	Tomasz Grabowski	Chapter 4.4
0.17	09/08/2013	Eray Özmü	Added Conclusion chapter 5
0.18	12/08/2013	Christoph Busold	Chapter 4 introduction
0.19	20/08/2013	Tomasz Grabowski Christoph Busold Detlef Houdeau	Overworked version after 1st review cycle
0.20	17/09/2013	Nuria Ituarte Aranda	Complete chapter 2.1 and 3.1

0.21	21/10/2013	Christoph Busold	Revised platform requirements in 4.2
0.22	21/10/2013	Frank-Michael Kamm	Revised Client requirements
1.00	30/10/2013	Maximilian Aigner Detlef Houdeau	Revised overall version

Table of Acronyms

AdES	**Ad**vanced **E**lectronic **S**ignature
AdES-A	**Ad**vanced **E**lectronic **S**ignature **A**rchival
AdES-C	**Ad**vanced **E**lectronic **S**ignature **C**omplete
AdES-T	**Ad**vanced **E**lectronic **S**ignature **T**imestamp
AdES-XL	**Ad**vanced **E**lectronic **S**ignature E**x**tended **L**ong-Term
ASiC	**A**ssociated **Si**gnature **C**ontainer
APS	**A**uthentication **P**rotocol **S**pecification
CAdES	**C**MS **Ad**vanced **E**lectronic **S**iganture
CMS	**C**ryptographic **M**essage **S**yntax
DoS	**D**enial **o**f **S**ervice
DoW	**D**escription **o**f **W**ork
ETSI	**E**uropean **T**elecommunication **S**tandards **I**nstitute
FS	**F**ederation **S**ervice
Gb/s	**G**iga**b**it / **s**econd
HDD	**H**ard **D**isk **D**rive
HTTP	**H**yper**t**ext **T**ransport **P**rotocol
HTML	**H**yper**t**ext **M**arkup **L**anguage
IE	**I**nternet **E**xplorer
iOS	**O**peration **S**ystem from Apple; Trademark

MAC	**Mac**intosh
OS	**O**peration **S**ystem
PAdES	**P**DF **Ad**vanced **E**lectronic **S**ignature
PC	**P**ersonal **C**omputer
PDA	**P**ersonal **D**igital **A**ssistant
PDF	**P**ortable **D**ocument **F**ormat
PKI	**P**ublic **K**ey **I**nterface
PR	**P**rivacy **R**equirements
RAM	**R**andom **A**ccess **M**emory
SAML	**S**ecurity **A**ssertion **M**arkup **L**anguage
SP	**S**ub **P**roject
SR	**S**ecurity **R**equirements
SSL	**S**ecure **S**ocket **L**ayer
STORK 2.0	**S**ecure iden**T**ity acr**O**ss bo**R**ders lin**K**ed, 2nd phase
TLS	**T**ransport **L**ayer **S**ecurity
TR	**T**echnical **R**equirements
TS	**T**echnical **S**pecification
XAdES	**X**ML **Ad**vanced **E**lectronic **S**ignature
XML	E**x**tensble **M**arkup **L**anguage

Table of Contents

1. Introduction

This document is concerned with the creation of general high level technical requirements for the whole FutureID infrastructure including server and browser as well as client components. This document starts with a system description which addresses all relevant technical components of the FutureID architecture.

The knowledge about existing eID credential systems would be used as written in D21.2 (Technical inventory) and in D32.1 (Survey and Analysis of existing eID and credential systems).

With D22.1 the technical framework will be defined to embrace potential future solutions based on more elaborate privacy-enhancing mechanisms. This could be achieved with a privacy enhanced authentication method. Privacy requirements (PR) will be addressed with D22.3, the related security requirement (SR) will be displayed in D22.2. The focus of this document, D22.1 will be on technical requirements (TR), which means high level functional aspects.

As terminology for the requirements the key words “MUST”, “SHOULD” and “MAY” are used.

1.1 **Scope of the document**

This document is only concerned with general technical requirements. There will probably be some overlaps with other requirements (e.g. security requirements, usability requirements etc.). The technical requirements will be concerned with the two main services (eSignature service and eID service). However low-level requirements are not subject of this document.

Furthermore only non-assurance related requirements will be stated in this document. Assurance related requirements will be created and documented in their respective interfaces (SP 3 and SP4) which will be determined by existing standards and are not subject of this document.

The basic functionality of each component is shown in the reference architecture which is displayed in D21.4.

1.2 **System Description**

An overview of the FutureID infrastructure is shown in Figure 1. The infrastructure in particular comprises the following components which will be described in this section:

- Client
- Identity Broker
- Universal Authentication Service
- Trust Repository
- Application Integration Services

A more complete description of the system components and their functionality can be found in the Description of Work (DoW) of the FutureID project.

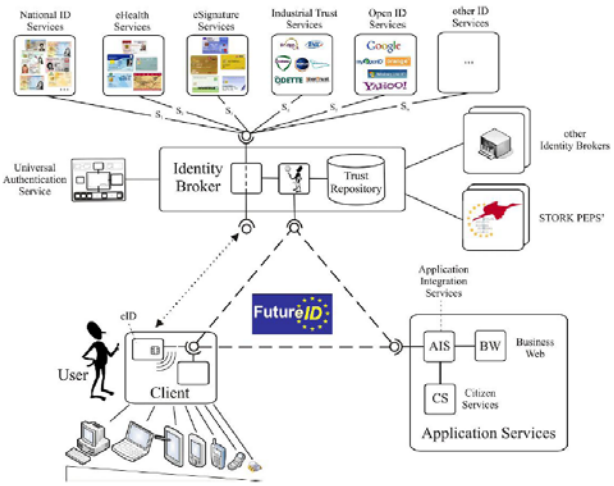

Figure 1 - General system architecture of FutureID showing the various system components and their interactions. Source: DoW

The interaction between each components of figure 1 is described in the reference architecture, see D21.4. Also the system service interface, the regular operations, the use cases as well as error states and procedures are displayed in D21.4.

1.2.1 Client

The client acts as an interface between the user (including any user-held eID hardware token) and the FutureID backend infrastructure. To facilitate the broad application of the FutureID technology, the client is designed to support all popular PC platforms and diverse mobile devices including notebooks, tablet PCs, PDAs, smart phones, other mobile phones and even other embedded devices.

1.2.2 Identity Broker

The Identity Broker will transfer eID information from the client side to the service provider and either works in the Dispatcher Mode, where it only serves as dispatcher and determines an appropriate authentication service, or in the Claims Transformer Mode, where it performs the

authentication itself (together with the attached Universal Authentication Service) and then transforms the claims to an appropriate protocol and credential, requested by the Service Provider.

1.2.3 Universal Authentication Service

The Universal Authentication Service is able to support all authentication protocols implemented by the various authentication tokens deployed across Europe. It makes it possible to support arbitrary authentication protocols by using a generic Execution Environment, which is capable of executing arbitrary protocols, which are described by appropriate Authentication Protocol Specification (APS) files. As the different authentication protocols are all composed of a rather limited set of basic cryptographic services, the problem of supporting arbitrary authentication protocols is reduced to providing this limited set of basic functionality and providing APS-descriptions for the different authentication protocols.

1.2.4 Trusted Repository

The Trust Repository is attached to the Identity Broker and provides a comprehensive repository for trusted certificates and services, SAML meta-data for trusted providers and other trust related information.

1.2.5 Application Integration Services

The Application Integration Services allow the communication between the appropriate Federation Service (FS) in the FutureID Infrastructure and the Application Services from the service provider.

1.2.6 System Boundary

The system components described above determine the system boundaries of the FutureID system and thus also the boundaries of the security considerations. On the other hand, this system architecture also determines the components which are outside the FutureID boundaries, namely

- user,
- the eID token hardware,
- issuer of the eID token
- the client hardware platform and software environment,
- the server and software infrastructure of the service provider who requests eID services from FutureID,
- the server and software infrastructure of an external identity provider.

While FutureID has external interfaces to these components, their security cannot be directly controlled by FutureID. FutureID will communicate with these components and services but can only control the security of a trusted communication channel on the side of the corresponding FutureID communication partner. It has to be assumed that cryptographic algorithms and communication protocols are implemented correctly on these external components and that their systems are in a trustworthy state (e.g. no malware on the server side or client platform).

Internal interfaces exist between the client and the identity broker, between the client and the application integration services and between the trust repository and the universal authentication service.

2. Technical Requirements on Services, Mandatory

The focus of this part is on all relevant high level technical and functional requirements for eID services and eSignature services, which are mandatory for a working mode in various use cases. Chapter 2.2 describes the eID services with the aspects of identification and authentication. Chapter 2.3 has the scope on eSignature services.

2.1 **eID Service**

The following general requirements for the eID Service provide a functional view on this specific service. More detail security specific requirements can be found in the respective deliverable document of D22.2 and on D32.2.

No.	TR-GEN-EID-01 General Compliance
Description	The eID service MUST comply with all service related requirements as written in D22.2 (security), D22.3 (Privacy), D22.4 (Usability), D22.5 (Socio Economics), D22.6 (Legal), D22.7 (accessibility) and D32.2 (eID Service).

No.	TR-GEN-EID-02 Technical Compliance
Description	The eID service MUST comply with all client related requirements as displayed in D31.1 (IFD), D32.2 (eID Service), D33.1 (eSignature), D34.1 (User Interface), D35.1 (Platform), D36.1 (Browser Integration) and D37.1 (Testbed).

No.	TR-GEN-EID-03 Restricted requests
Description	The eID service MUST restrict attribute requests to certify and authenticated relying parties.

No.	TR-GEN-EID-04 Secure login and logout
Description	The eID service MUST provide secure login and logout.

No.	TR-GEN-EID-05 Informed consent
Description	The eID service MUST offer user consent mechanisms in order to inform the user the information that is being transmitted as well as mechanisms to stop the transmission by the user.

No.	TR-GEN-EID-06 Data integrity
Description	The eID service MUST avoid user data changes (the votes, the answers to a survey, etc.) without user consent.

No.	TR-GEN-EID-07 Attribute checking
Description	The eID service MUST avoid providing false values for attributes that are required.

No.	TR-GEN-EID-08 Anonymity and pseudonymity
Description	The eID service MUST provide mechanisms for anonymous authentication as well as the possibility of using pseudonyms. The linkage of pseudonyms to real identities will only be performed with user consent.

No.	TR-GEN-EID-09 Minimal disclosure
Description	The eID service MUST provide mechanisms for avoiding the disclosure of unnecessary user information that is only the relevant information for the transaction must be revealed.

No.	TR-GEN-EID-10 Avoid duplicated votes
Description	For votes and polls the eID service MUST provide mechanisms for avoiding that a particular person has participated already.

No.	TR-GEN-EID-11 Protocols support
Description	The eID service MUST support various eID services and different authentication protocols. And also the eID service must allow the possibility of adding more authentication protocols.

No.	TR-GEN-EID-12 Support of authentication servers
Description	The eID service MUST support various authentication services and one of these authentication services will be selected. The following means of authentication can be supported according to D41.1: • eID-servers • STORK-PEPS • eID Broker • polish government • Austrian MOA-ID server • Estonian Mobile • Facebook using OAuth 2.0

	• Linkedin using OAuth 2.0 • XING using OAuth 1.0 • Attribute-based Credentials based on Idemix, U-Prove or alternative constructions.

No.	TR-GEN-EID-13 Different platforms
Description	The eID service MUST support any technical customer platform available (PC, tablet, smartphone).

No.	TR-GEN-EID-14 Deactivate eID
Description	The eID service MUST provide mechanisms for deactivate or revoke the eID requested by the user (due to a lost or theft).

No.	TR-GEN-EID-14.1
Description	The eID service MUST be deactivated if the user reports a loss, which needs to be authenticated to prevent DoS.

No.	TR-GEN-EID-14.2
Description	The eID service MUST be deactivated if authorities revoke a card to maintain security.

No.	TR-GEN-EID-15 Personally Identifiable information protection
Description	The eID service MUST provide mechanisms for protecting any personally identifiable information transmitted or processed.

No.	TR-GEN-EID-16 No authorized access to log files
Description	The eID service MUST provide mechanisms for avoiding access of unauthorized persons to the log files.

No.	TR-GEN-EID-16.1 Limitation of logging
Description	The eID service MUST limited the logging procedures.

No.	TR-GEN-EID-17 Integrity of transported messages
Description	The eID service MUST provide mechanisms for preserving the integrity of the transported messages.

No.	TR-GEN-EID-18 High Availability
Description	The eID service MUST support high availability and fault tolerance.

No.	TR-GEN-EID-19 Error Handling
Description	Error handling or exception states MUST be supported.

2.2 eSignature Service and Signature Validation

The following general requirements for the eSignature Service and the Signature validation provide a functional view on this specific service. More detail security specific requirements can be found in the respective deliverable document of D22.2 and on D32.2 as well as on D33.1.

No.	TR-GEN-ESI-01 General Compliance
Description	The eSignature service MUST comply with all service related requirements as written in D22.2 (security), D22.3 (Privacy), D22.4 (Usability), D22.5 (Socio Economics), D22.6 (Legal), D22.7 (accessibility), D32.2 (eID Service) and D33.1 (eSignature Service).

No.	TR-GEN-ESI-02 Technical Compliance
Description	The eSignature service MUST comply with all client related requirements as displayed in D31.1 (IFD), D32.2 (eID Service), D33.1 (eSignature), D34.1 (User Interface), D35.1 (Platform), D36.1 (Browser Integration) and D37.1 (Testbed).

No.	TR-GEN-ESI-03 Signature
Description	The eSignature service MUST support the secure signing of documents as defined in D33.1.

No.	TR-GEN-ESI-03.1 Trusted Path for Signature
Description	The system MUST support a trusted viewing path for signatures and integration of a PIN entry at a secure terminal.

No.	TR-GEN-ESI-03.2 Signing Token
Description	The eSignature service MUST support at least one of the following electronic signatures: a) SW-signature b) Smart Card signature c) Mobile Signature using secure elements in mobile phones or d) Mobile Signature using server signing.

No.	TR-GEN-ESI-03.2.1 PDF Signature
Description	The eSignature service MUST support PDF-Signatures and PAdES along ETSI TS 102 778. Code infusion in the time window between signing and verification MUST be preventing.

No.	TR-GEN-ESI-03.2.2 Multiple Token
Description	The eSignature service MUST support multiple citizen eID-cards and other token as descript in TR-GEN-ESI-03.1.

No.	TR-GEN-ESI-03.2.3 No Restriction
Description	The eSignature service MUST avoid any kind of restrictions on the type of document signed.

No.	TR-GEN-ESI-03.3 Signature Validation
Description	The eSignature service MUST comply with the signature validation process as descript in D32.2.

No.	TR-GEN-ESI-03.4 Anonymus Credential
Description	The eSignature service MUST support anonymous credential based attribute signatures on documents.

3. Technical Requirements on Services, Optional

The focus of this part is on all high level technical and functional requirements for eID services and eSignature services, which are optional for a working mode in various use cases. Chapter 3.2 describes the eID services with the aspects of identification and authentication. Chapter 3.3 has the scope on eSignature service.

3.1 **eID Service**

No.	TR-GEN-EID-19 Errors Management
Description	It's RECOMEMNDED for eID services to perform error handling including sufficiently detailed error information.

No.	TR-GEN-EID-20 Error messages and logs
Description	The eID service SHOULD display transaction error messages for informing the user as well as register logs with transactions information in the system components.

No.	TR-GEN-EID-21 History function
Description	The eID service SHOULD provide mechanisms to show a history of recent transactions of the active user as well as mechanisms to delete history in FutureID components.

No.	TR-GEN-EID-22 Different trust models
Description	The eID service SHOULD support different trust models (PKI, Trusted Lists and Trust Status Lists).

No.	TR-GEN-EID-23 Support for identity management protocols
Description	The eID service SHOULD support Identity Management Protocols SAML 2.0 and OpenID 2.0 for exchanging authentication data.

No.	TR-GEN-EID-24 Support for transmitting, exchanging or binding credentials
Description	The eID service SHOULD support for transmitting or exchanging credentials and also for binding credentials (e.g. to other credentials, device or eID application).

No.	TR-GEN-EID-25 Support for transmitting, exchanging or binding credentials
Description	The eID service SHOULD support for transmitting or exchanging credentials and also for binding credentials (e.g. to other credentials, device or eID application).

No.	TR-GEN-EID-26 Support for authentication protocols
Description	The eID service SHOULD cover the authentication protocols supported by the existing eID cards identified in D32.1. This includes the following protocols: * EAC protocol * RSA Authentication protocol * Mutual authentication protocol * TLS protocol In addition the following protocol MAY be supported: * CIPURSE v2 mutual authentication and key agreement protocol

No.	TR-GEN-EID-27Trust services
Description	The eID service SHOULD allow the use of the services belonging to the Trust Service.

3.2 eSignature Service

No.	TR-GEN-ESI-03.3
Description	The eSignature service SHOULD support CMS and CadES according ETSI TS 101 733.

No.	TR-GEN-ESI-03.4
Description	The eSignature service SHOULD support XML and XadES according ETSI TS 101 903.

No.	TR-GEN-ESI-03.5
Description	The eSignature service SHOULD support long term forms like AdES-T/-C/-XL and –A.

No.	TR-GEN-ESI-03.6
Description	The eSignature service SHOULD support ASiC along ETSI TS 102 918.

No.	TR-GEN-ESI-03.7
Description	The eSignature service SHOULD support different trust models, such as PKI or Web of Trust.

No.	TR-GEN-ESI-03.8
Description	The eSignature service SHOULD support different signatures, such as proxy signature, blank signature and blind signature.

No.	TR-GEN-ESI-03.9
Description	The eSignature service SHOULD support trusted lists and trusted status lists as trust anchor distribution format.

No.	TR-GEN-ESI-03.10
Description	The trust settings of the eSignature service can be assumed other trusted users.

No.	TR-GEN-ESI-03.11
Description	The eSignature service SHOULD support STORK 2.0 for cross border signatures and delegation.

No.	TR-GEN-ESI-03.12
Description	The eSignature service SHOULD support a validation with understandable user feedback in case of failed validation.

4. Technical Requirements on Platform

Chapter 4 discusses the technical requirements of FutureID on the involved platforms. This chapter focuses on a high-level description of the requirements. Some sections have related deliverables with a more detailed requirements analysis in their context, like D35.1 for the client platform and D36.1 for browser integration.

This chapter is structured as follows. Section 4.1 describes the general requirements for platforms on which the FutureID client is running. Technical requirements for the browser platform, including its integration with the FutureID client, are detailed in section 4.2. Finally, section 4.3 discusses the requirements for servers which are part of the FutureID backend infrastructure.

4.1 **Client Platform**

The FutureID client is one of the central components of the FutureID architecture, since it provides a direct interface to the user, to external eID hardware tokens, to the service provider, to an external identity provider and to the FutureID server backend. From a user perspective it is therefore the entry point to federated identity management with FutureID and will be a central factor of user acceptance of the whole FutureID concept.

From the security and privacy point of view, the client is also in a key position since it provides the highest number of interfaces of all FutureID components, interacts directly with the actual eID tokens and runs on a user platform with unknown security properties. Due to the direct user interaction, aspects like accessibility, inclusion and usability will be mainly determined by the client properties.

The following general requirements for the client provide a more functional view on the main client properties. More detailed specific technical requirements, referring to actual implementation options and compliance with specific standards and specifications can be found the respective deliverable documents of SP 3 for each client module.

No.	TR-GEN-CLI-01 General Compliance
Description	The client MUST comply with all client-related requirements of deliverables D22.2 (Security), D22.3 (Privacy), D22.4 (Usability), D22.5 (Socio Economics), D22.6 (Legal), D22.7 (Accessibility and Inclusion).

No.	TR-GEN-CLI-02 Technical Compliance
Description	The client MUST comply with all client-related requirements of SP3-deliverables, especially D31.1 (IFD), D32.2 (eID), D33.1 (eSignature), D34.1 (User Interface), D35.1 (Platform), D36.1 (Browser Integration) and D37.1 (Testbed).

No.	TR-GEN-CLI-03 Sessions
Description	The client MUST be able to establish a secure session communication (according to D22.2) with the service provider, the FutureID backend and external identity providers.

No.	TR-GEN-CLI-04 Authentication
Description	The client MUST provide the functionality to perform authentication to the FutureID backend, to a service provider, to a hardware token and to an external identity provider.

No.	TR-GEN-CLI-05 Federation
Description	The client MUST support identity federation between an identity provider and the FutureID Identity Broker and between the service provider and the FutureID Identity Broker.

No.	TR-GEN-CLI-06 Signature
Description	The client MUST be able to securely sign documents according to deliverable D33.1.

No.	TR-GEN-CLI-07 Tokens
Description	The client MUST support secure communication with all hardware tokens (e.g. smart cards) used within the EU for official electronic identification and with all hardware tokens developed within the FutureID project. The client MUST therefore support all standards and protocols as specified in D32.2.

No.	TR-GEN-CLI-08 Interfaces
Description	The client MUST provide interfaces to the FutureID backend, to the user, to the service provider, to eID hardware tokens and to external identity providers.

No.	TR-GEN-CLI-09 User Interface
Description	The client MUST provide a graphical user interface that allows the user to control the authentication process, to obtain security and privacy related information, to choose the authentication method (if applicable), to be informed about the progress and status of the authentication, to stop the authentication if desired, to enter login credentials and to perform signatures. The user interface MUST therefore especially be compliant with the deliverables D22.4 (Usability) and D22.7 (Accessibility and Inclusion).

No.	TR-GEN-CLI-10 Plattforms
Description	The client MUST be available on PCs and mobile devices (smart phones, tablet computers) supporting at least the most popular operating systems (e.g. Windows, Linux, MAC OS, Android, iOS). It SHOULD therefore be implemented in a platform-independent language like Java.

No.	TR-GEN-CLI-11 Open Source
Description	The client software MUST be available under Open Source license.

4.2 **Browser**

In this section, we specify the technical requirements for the browser in the FutureID architecture and its integration into the FutureID client.

FutureID should be integrated into web applications. This of course requires a browser application, which supports common standard functionality. Besides basic HTTP protocol support and HTML rendering, this includes client-side scripting with JavaScript, storage of session cookies on the client platform and support for SSL/TLS secure channels. Browser-based federated identity management protocols use cookies to store authentication tokens, or even exchange them between the websites of identity and service provider. The support for cookie-less browsers is desired but optional.

No.	TR-GEN-BRO-01 Standard Web Browser Support
Description	The browser platform of the FutureID user MUST support all standard web browser functionality.

Since there is a variety of different operating systems and browsers, the browser-related parts of the FutureID infrastructure should make use of standard web browser functionality as far as possible. This allows FutureID to achieve a high level of platform independence.

No.	TR-GEN-BRO-02 Standard Functionality
Description	Browser-specific parts of FutureID SHOULD be based on standard web browser functionality as far as this is possible.

The browser integration has to support all platforms targeted by the FutureID client as specified in D37.1 Requirements Report Client Testbed. On desktop systems these include the operating systems Windows, Mac OS and Ubuntu Linux as well as the browsers Internet Explorer, Firefox, Safari and Chrome. Support for further platforms is desired, but will not be tested.

No.	TR-GEN-BRO-03.1 Supported Desktop Platforms and Browsers
Description	FutureID MUST support Internet Explorer (IE), Firefox and Chrome on Windows 7 and Windows 8, Safari and Firefox on Mac OS 10.8 and Firefox on Ubuntu Linux. It SHOULD support Firefox on other Linux distributions, and further MAY support Opera on Windows, Mac OS and Linux. The oldest available version SHOULD be supported, like Firefox V17, Safari V4, Chrome V23.0, Opera V12.2 and Explorer V10.0. FutureID would be foster browser independent solution.

On mobile devices, FutureID must support at least the popular Android operating system with Chrome as specified in D37.1 Requirements Report Client Testbed. Other mobile platforms like iOS and Windows Phone should be supported, but will not be tested.

No.	TR-GEN-BRO-03.2 Supported Mobile Platforms and Browsers
Description	FutureID MUST support devices with Android operating system version 4.1 and Chrome as browser. It further SHOULD support newer Android versions 4.2+ as well as iOS and Windows Phone with their standard browsers. Support for other browsers on mobile devices is OPTIONAL.

In order to authenticate on a FutureID supported website, there has to be a communication channel between the browser and the FutureID client. This requires some form of browser integration.

No.	TR-GEN-BRO-04 Browser Integration
Description	The FutureID infrastructure MUST provide communication channel between the Browser and the FutureID Client.

The requirements for such a browser integration as well as possible solutions will be evaluated in more detail in deliverable D36.1. Therefore the following requirement should be substituted by the requirements defined in the referenced document.

No.	TR-GEN-BRO-05 Browser Integration Compliance
Description	The FutureID infrastructure MUST comply with all technical requirements for such a browser integration solution defined in D36.1 (Requirements Analysis for Browser Integration).

The FutureID client should further support multiple concurrent web sessions, which use FutureID for authentication.

No.	TR-GEN-BRO-06 Multiple Sessions
Description	The FutureID client and the browser SHOULD support multiple FutureID authenticated sessions at the same time.

No.	TR-GEN-BRO-07 Session Compatibility
Description	FutureID sessions MUST NOT interfere with the sessions of other web applications.

4.3 Server

Servers are an essential part of every IT solution. There are also the important issues of the FutureID project. The appropriate selection and adaptation to needs of the project helps to achieve user satisfaction and reduces frequent intervention in the infrastructure. The FutureID project aims to build a sophisticated server infrastructure to integrate with the client in order to ensure secure and user satisfaction as well as fast and stable infrastructure.

One of the key technical requirements in FutureID project is server's scalability and ensure to their adequate load balancing. In this case we should consider two quite different approaches.
The first one is based on single computing server room solution with additional second geographically separated server room site to support unavailability of first server room access (High Availability Active-Passive solution). This solution is based on few dedicated servers with separated disk matrix with full redundancy on second site (geographically separated server room). To achieve High Availability Active-Active mode (commonly known as load balancing) internal structure of server room must be designed with respect to computer software which also should be thread enabled and ready to be scattered at least at multithread level. Architecture of connections between servers depends on algorithms chosen to scatter computing. By default configuration we should consider at least server cluster, build using few machines connected with high speed network (1 or 10 Gb/s), logically separated as Active-Passive nodes. In this case scalability can be done easily by adding two more nodes to current active-passive cluster.

The second approach is significant different. It is based on distributed environment. Many servers with small computational power (i.e. 2 servers in Active-Passive mode with internal storage) but very scattered environment can be used when number of transactions expected to be processed per second is very high but transactions will be not very computational requiring. Each request will be sent to master node and then scattered to all nodes available in each localisation. In this case scalability can also be easily done by adding new cluster with new geographically location (2 servers in Active-Passive mode). Communication between nodes in this solution can base on Tyrant's Algorithm or Map Reduce or alternatives. One of those algorithms should be implemented also in software because classic approach (parallel threads) cannot be used in distributed environment.

In this section the technical requirements for the servers in the FutureID architecture is shown. The following general requirements present main functional properties of the server infrastructure. More detailed technical requirements can be found in SP 3 and SP 4 deliverable documents.

No.	TR-GEN-SER-01 Network card
Description	Network card / network cards set MUST provide access to the server or ensure waiting time no longer than previously defined.

No.	TR-GEN-SER-02 Processors
Description	The FutureID infrastructure MUST be based on multi-core processor server machines to scatter server overload together with thread enabled software.

No.	TR-GEN-SER-03 RAM allocation
Description	After running the server software it SHOULD be available at least 20% of free RAM to be used by software or software SHOULD allocate the maximum available memory during start up process.

No.	TR-GEN-SER-04.1 HDDs / disk arrays
Description	Processing servers and logical processing machines MAY have fast and low capacity hard drives (software binaries are not frequently changed and not disk space required).

No.	TR-GEN-SER-04.2 HDDs / disk arrays
Description	The providing redundancy external storages / disk arrays (at least mirror) SHOULD be the best practices in the servers involved in the data processing (DBs).

No.	TR-GEN-SER-05 Disk array – server connections
Description	Hardware disk array MUST be connected to the server using high-speed network (i.e. 10 Gb/s).

No.	TR-GEN-SER-06.1 Connections between servers
Description	In centralized solution connection between servers SHOULD be at least 1 Gb/s Ethernet to avoid unnecessary delays with independent network collision domain.

No.	TR-GEN-SER-06.2 Connections between servers
Description	In distributed environment connection between servers SHOULD be faster than connection from client workstation to processing servers.

No.	TR-GEN-SER-07.1 Hardware
Description	The hardware use-cases MUST depend on the scale of the FutureID project. Important for centralized solutions is the quality (speed connections) between storage arrays and servers.

No.	TR-GEN-SER-07.2 Hardware
Description	The hardware use-cases MUST depend on the scale of the FutureID project. For distributed solutions more essential than the speed of disks are a number of nodes and the way of communication between them (communication algorithms in distributed environment).

No.	TR-GEN-SER-08 Copy the environment
Description	In the case of a centralized solution server administrator MUST ensure a copy the environment in geographically independent location (geographically independent sites) as the *HA Active/Active* or at least *HA Active/Passive* configuration.

No.	TR-GEN-SER-09 Active threads and logical cores of the server
Description	The total number of application active threads running on server SHOULD not be higher than the number of logical server cores.

No.	TR-GEN-SER-10 Backup application politics running on a server
Description	Server and application configuration backup policies MUST be set at least before the stage of installing the test version.

No.	TR-GEN-SER-11 Backup
Description	The backups MUST reproduce a fully functional environment with the respect to the nearest performed backup based on and their properties (incremental, differential, comprehensive, etc.).

5. Conclusion

The technical requirements of FutureID are very important for the success of the whole services and the underlying infrastructure. This document has successfully described the most important requirements on a high level. We recommend strictly orienting towards these requirements in the following works.

By following these requirements a flexible and ubiquitously usable infrastructure for secure authentication across borders will be possible. It is highly recommended to focus on MUST requirements first and set priorities according to the requirement level.

6. Bibliography

N/A