D41.6

Legal analysis of the FutureID Broker[1]

Document Identification	
Date	29/10/2015
Status	Final
Version	Version 1.0

Related SP / WP	SP4/ WP41	**Document Reference**	D41.6
Related Deliverable(s)	D12.9, D32.8, D33.6, D41.1, D41.2	**Dissemination Level**	PU
Lead Participant	KUL	**Lead Author**	Jessica Schroers
Contributors	Jessica Schroers (KUL) Colette Cuijpers (RU) Hannah Obersteller (ULD) Pedro Malaquias (KUL)	**Reviewers**	Alfredo Rial (IBM) Juan Carlos Pérez Baún (ATOS)

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.

[1] The original title “Legal analysis of the Identity Broker” has been adjusted due to terminology changes during the project.

1. Executive Summary

This deliverable provides an analysis of the legal framework surrounding the FutureID Broker as a legal entity, with a special focus on liability.

The deliverable starts with an introduction to the FutureID Broker and the FutureID Ecosystem. This is followed by an explanation of the importance of liability within the identity management context as an enabler of trust. The section provides a high-level conceptualization of the various expectations held by the different entities that participate in FutureID.

The main part of this deliverable gives an overview of the different sources of liability and how they could apply to the FutureID Broker. First an overview of non-contractual liability, resulting from Data Protection law, e-signature/eIDAS legislation and tort law. For data protection law, the distinction between controller and processor remains important. In case the FutureID Broker is a controller, it will be subject to more stringent obligations and, hence, a higher risk for liability. On the other hand, if the FutureID Broker is simply a processor, it shall be subject to less onerous obligations, although it might still face liability claims. Depending on the national implementation of the data protection law, the FutureID Broker as a processor could be held directly liable, or indirectly via contractual clauses in the controller-processor contract by the controller/SP.

The legislation on electronic signatures changed, and was broadened under the eIDAS Regulation. It also covers other trust services and notified identity services. In this regard, the risk of liability is lower for the FutureID Broker, as with its current service profile it does not qualify as a certification service provider/trust service provider in the sense of the legislation. The role of Brokers such as the FutureID Broker is not specifically considered under the eIDAS Regulation. If the FutureID Broker would receive an assertion from a national operator of the authentication procedure, based on a notified eID, the FutureID Broker as a legal entity in Claims Transformer Mode could be considered a relying party. In this case, the eIDAS provision might give the FutureID Broker some rights vis-à-vis the party issuing the electronic identification means, the party operating the authentication procedure or the notifying Member State. Nevertheless it has to be taken into account that the rules are aimed at public services and that the Regulation leaves the choice to accept private relying parties to the Member States, including the possibility to define terms of access, which could entail liability limitations.

Tort law varies substantially between Member States, but usually requires a fault, a damage and a causal connection between the fault and the damage. It will often be difficult for the user and the SP to demonstrate that they suffered a material damage. Non-material damage can be awarded, but the judges are reluctant in this regard. Taking into account the heightened importance of data, this might possibly change in the future. The characterisation of the fault is another difficulty, as it is not yet clear which rights and obligations the FutureID Broker has. However, obligations could result from legislation such as data protection law, applicable standards but also contracts. In case of contracts the failure to

comply with contractual obligations could possibly not only give rise to pre-defined contractual liability, but also to tort liability, depending on the national law.

The contractual liability will depend on the exact provisions in the contracts. The reference architecture envisages a strongly decentralized deployment. This would entail that every participant of the FutureID ecosystem would enter into contracts with the party they rely upon, and, as part of their contractual freedom, can decide on the contract provisions. This will most likely result in a chain of contracts. As such, it is important that the FutureID Broker enters into back-to-back liability arrangements to ensure that no gap in liability coverage exists, leaving the Broker with uncovered risks. In particular in case of usage of a single trade mark or distinctive sign, it might be advisable that a governing entity would establish and (possibly) enforce obligations for the different participants. Points which should be considered in the contracts are the role and responsibilities of each partner, the applicable law, dispute resolution and which liabilities are accepted towards each stakeholder (including financial limitations). The contracting partners should also consider Service Level Agreements and provide for obligations to implement and follow inputs and instructions from the governing entity. Finally they should cover the data protection requirements, e.g. by controller-processor contracts.

To complete the analysis, the position of the FutureID Broker under the Directive 2000/31/EC is assessed. The provisions of this Directive seem to apply as the FutureID Broker will probably provide an information society service. However, it does not seem likely that the FutureID Broker can benefit from the liability exemptions. An exception might be the Broker in Dispatcher Mode, who might be able to invoke the exemption of mere conduit (this is however disputable). As the FutureID Broker will not provide a hosting service, it is clear that the exemptions of caching and hosting are not applicable.

Finally the analysis concludes with a case study on failures in authentication systems in the Netherlands. These examples show that the risk of liability claims is currently not high and can be countered with limited liability clauses. However, a bigger risk seems to be the loss of trust.

It is advisable that the FutureID Broker establishes adequate liability limitations and back-to-back liability arrangement, while at the same time ensuring the trust between all the parties. This could include the provision of simple redress mechanisms and support and contact points. Users should have support when problems arise and it should be avoided to oblige users to prove what went wrong in a system they do not understand. Finally, logging is useful, as it can provide evidence in the question whose fault the failure was, and therefore facilitate getting redress from the liable party.

2. Document Information

2.1 Contributors

Name	Partner
Jessica Schroers	KUL
Colette Cuijpers	RU
Hannah Obersteller	ULD
Pedro Malaquias	KUL

2.2 History

Version	Date	Author	Changes
0.1	12.05.2015	Jessica Schroers	First draft
0.2	04.10.2015	Jessica Schroers, Bud Brügger	Second draft, including section 5.1.
0.2	07.10.2015	Colette Cuijpers, Hannah Obersteller	Review + additional information
0.3	27.10.2015	Jessica Schroers	Version for review
1.0	29.10.2015	Jessica Schroers	Final version

2.3 Table of Acronyms

BGB Bürgerliches Gesetz Buch (German Civil Code)

BS Broker Service

CI Credential Issuer

CSP Certification Service Provider

EU European Union

ID number Identity number

IdP Identity Provider

LoA Level of Assurance

PKI PKI Public Key Infrastructure

SAML Security Assertion Markup Language

SP Service Provider

2.4 Referenced documents

Literature

J. Alhadeff, B. van Alsenoy, et.al., "Legal and Policy handbook for TAS^3 implementations", TAS^3 Deliverable D6.1-2, v.1.0, January 2012.

B. Van Alsenoy, E. Lievens, K. Janssen, J. Dumortier, K. Rannenberg, S. Yang, T. Andersson, Q. Abbas, H. Leitold, B. Zwattendorfer, "A Regulatory Framework for INDI Operators", GINI deliverable 3.2., 27.4.2012.

B. van Alsenoy, "Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC", Computer law & security review 28 (2012), pp. 25-43.

P. Balboni, "Liability of CSPs towards relying parties and the need for a clear system to enhance the level of trust in electronic communication", Information&Communications Technology Law, Carfax Publishing, Vo.13, No.3, 2004.

C. von Bar, U. Drobnig, *The Interaction of Contract Law and Tort and Property Law in Europe – A Comparative Study*, Sellier.European Law Publishers, München, 2004.

C. Bastos, M. Drabik, D. Hühnlein, T. Hühnlein, N. Ituarte, A. Lehmann, G. Neven, J. Schmölz, C. Rath, "D41.2 Interface and module specification and documentation", FutureID deliverable v1.1, 11.12.2013.

G. Borges, „Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis - Ein Gutachten für das Bundesministerium des Innern", 2010, p.199, available at: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/PaesseAusweise/rechtsfragen_npa.html

C. van Dam, *European Tort Law*, Oxford University Press, 2013.

G. Dimitrov, *Liability of Certification Service Providers*, PhD thesis, KU Leuven, 2007.

J. Dumortier, N. Vandezande, "Trust in the proposed EU regulation on trust services?", *Computer Law and Security Report.* nr.28 , 2012, pp. 568-576.

M. Ebers, A. Janssen, O. Meyer (ed), *European Perspectives on Producers' Liability*, sellier.european law publishers, 2009.

Gola/Klug/Körffer in Gola/Schomerus, *BDSG - Bundesdatenschutzgesetz*, C.H. Beck, München, 2012.

H. Graux, "D3.1. – Legal Needs Analysis Report", STORK2.0 deliverable, 8.5.2013.

Jandt, „Beweissicherheit im elektronischen Rechtsverkehr – Folgen der europäischen Harmonisierung", NJW 2015, 1205.

D. Korff, "Working Paper No. 2 – Data Protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments", Comparative study of different approaches to new privacy challenges, in particular in the light of technological developments, European Commission – DG JFS, 20.1.2010.

Lodder and H.W.K. Kaspersen (ed.), "eDirectives: Guide to European Union Law on E-Commerce", The Hague, Kluwer, 2002.

U. Magnus, 'Comparative Report on the Law of Damages', in u. Magnus (Ed.), *Unification of tort law: damages*, Principles of European Tort Law Volume 5, Kluwer, 2001, pp. 185-217.

J. Spier and O. A. Haazen, "Comparative Conclusions on Causation", in J. Spier (Ed.): *Unification of Tort Law: Causation*, Kluwer, 2000.

T. Wich, D. Hühnlein, J. Schmölz, D41.1 Requirements report, FutureID deliverable v1.1., 11.12.2013.

P. Widmer, "Comparative Report on Fault as a Basis of Liability and Criterion of Imputation (Attribution)", in P. Widmer (Ed.), *Unification of Tort Law: Fault*, Kluwer, The Hague, 2005.

Legislation and case law

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the European Union, L 257/73, 28.8.2014, (eIDAS).

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)., e-commerce Directive).

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal of the European Union, L 13, 19.1.2000.

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, Official Journal of the European Union, L 281, 23.11.1995.

Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens).

Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 25. Februar 2015 (BGBl. I S. 162) geändert worden ist"; neugefasst durch Bek. v. 14.1.2003 I 66; zuletzt geändert durch Art. 1 G v. 25.2.2015 I 162; (BDSG).

BGH Urteil VI ZR 33/81 29.6.1982.

Vidal-Hall & Ors v Google, EWCA Civ 311 Court of Appeal 2015.

Commission Implementing Regulation (EU) 2015/1502.

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 application services 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. Outline and scope

This deliverable provides an overview of liability in identity management systems, specifically for the FutureID Broker in the FutureID system. As the Broker service is a technical component, a legal analysis would not yield many results. Therefore the FutureID Broker and its role in the bigger ecosystem, as envisaged in the reference architecture, will be analysed and legal considerations be outlined.

Section 5 describes the FutureID Broker and the FutureID Ecosystem. Section 6 explains the importance of liability in an identity management context, and the risks and stakeholder expectations in the FutureID system. Section 7 provides an overview of sources of liability and whether possible liability exceptions of Directive 1999/93/EC might be invoked by the FutureID Broker. The main part of the analysis can be found in this section, where the different sources of liability (legal obligations, tort and contracts) are examined. Finally an example of failures within identity management systems in the Netherlands is presented, to show whether and how liability risks up until now have realised in practice.

6. The FutureID Broker

A FutureID Broker is a legal entity which provides the FutureID authentication service. The FutureID authentication service is a service which allows users to authenticate themselves towards Service Providers (SP) using pre-existing credentials. The technical component which makes this possible is referred to as the "Broker Service" (BS).

The Broker Service can operate in two modes, Dispatcher and Claims Transformer Mode. In the Dispatcher Mode, the Broker Service only serves as a dispatcher, meaning that it determines an appropriate Authentication Service, which performs the authentication of the user and returns the result of the authentication to the requesting SP.[2] In this mode the Broker Service does not sign any assertion or credential but simply serves as a proxy.[3] The Claims Transformer Mode can be seen as an extension of the Dispatcher Mode, where the Broker Service transforms the externally authenticated attributes into a new credential or token.[4] The Claims Transformer Mode can have different settings. The simplest form will issue a short-lived token to the SP, e.g. using SAML-assertions, while in a more advanced setting the Broker Service can issue long-term privacy-enhancing attribute-based credentials (Privacy-ABCs) to the user.[5]

The Broker Service can be implemented as a technical component at the SP's side, but can also be provided by a separate legal entity, i.e. a FutureID Broker.

6.1 The FutureID Ecosystem[6]

The different stakeholders of the FutureID Ecosystem have been described in D32.8, Section 6 and 7. For this analysis, we will describe potential relations and scenarios between the different stakeholders. It is assumed that the user possesses one or more credentials issued by the legal entity "issuer". The user would like to access a service provided by the legal entity "SP". The SP outsourced the authentication to the legal entity "FutureID Broker", who operates the technical component BS (Broker Service).

1.) The FutureID Broker can offer its services in dispatcher mode

2.) The FutureID Broker can offer its services in claims-transformer mode

[2] D41.1, p. 4.
[3] D41.1, p.4.
[4] D41.2, p. 41.
[5] D41.2, p.41.
[6] Based on information of Bud Brügger.

When the FutureID Broker operates in claims-transformer mode, it could be possible that either (a) the FutureID Broker is capable of verifying the credential directly (by operating a software component such as the UAS) or (b) the FutureID Broker requires the service of the legal entity "IdP" (Identity Provider)[7].

In (a), the FutureID Broker is responsible for remote verification of the credential, including the (possibly cryptographic) verification of the credential and the extraction of identity attributes (data) from the credential. The FutureID Broker would then issue a signed assertion that contains identity attributes of the user (possibly filtered) and is sent through a user component (executor or browser) to the SP.

In (b) the FutureID Broker redirects the user to the IdP, who is responsible for the remote verification of the credential and for issuing a signed assertion that is sent (through a user component) to the FutureID Broker. The FutureID Broker verifies this assertion (e.g., the signature) and that it comes from a trusted IdP (based on the IdPs certificate that signed the assertion). Then it extracts the user's identity attributes from the assertion, and issues a new assertion that contains (a subset of) identity attributes which will be signed by the FutureID Broker. The second assertion is sent through a user component to the SP.

Both scenarios in the Claims Transformer Mode can again happen in two different versions: either the user has the FutureID Client installed, or the user relies on the FutureID Broker ('User-Broker'). If the user has a FutureID Client and an Executor installed, the user is in full control of passing the credential/assertions to IdP, Broker, and SP, respectively. The user also asks the Broker to issue a new assertion based on the one from the IdP. This means, there is no direct interaction between the IdP and the Broker, and between the Broker and the SP, but solely directly between the user and these legal entities. If the user is given appropriate information and then explicitly agrees to the data processing (depends on the user interface), the user has provided consent to the interactions with these legal entities. If the user has only a browser and, therefore, relies on a User-Broker, the user will generally choose the User-Broker and have an account there. Data processing would be allowed as there would be a contract between the user and the User-Broker, providing consent for the processing. The User-Broker does not necessarily need to be different from the FutureID Broker connected to the SP. The User-Broker lets the user choose an authentication plan that determines: the credential to be used, in case (2.b) the IdP to contact, in all cases the Broker to contact, and the SP.

[7] The IdP can be the same entity as the issuer, but can also be a separate entity.

7. Liability in IdM context

Trust is important for a functioning market place. This importance is referred in the first recital of the eIDAS Regulation[8], stating that:

> "*Building trust in the online environment is key to economic and social development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services."*

One important factor in establishing or increasing trust is the existence of a clear and effective system of liability.[9] In general people trust the rule of law and the idea that "if anything goes wrong 'someone will be liable' for the damage caused to their property as a result of the other party's misconduct".[10] Therefore, trust can be promoted with the presence of a clear liability regime.[11] This system should be "understandable, user-friendly, coherent and clear as to the responsibilities its rules impose and the conditions applied for the recovery of compensation".[12]

Liability can on the other hand also establish a market barrier. Strict liabilities can have chilling effects, and high requirements which demand substantial investments to comply with them (such as audits) may augment a barrier and decrease the market accessibility.[13]

7.1 Liability risks and stakeholder expectations

In a complex technical system, there are many things that can go wrong. Faulty identification or authentication, inadequate security and misuse of personal data, failure to follow appropriate procedures, may each give rise to liability.[14]

---

[8] Regulation (EU) No 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS).
[9] Dimitrov p. 41.
[10] G. Dimitrov, "Liability of Certification Service Providers", PhD thesis, KU Leuven, 2007, p.86, referring to Balboni, Liability of CSPs towards relying parties and the need for a clear system to enhance the level of trust in electronic communication, Information&Communications Technology Law, Carfax Publishing, Vo.13, No.3, 2004, p.217.
[11] G. Dimitrov, "Liability of Certification Service Providers", PhD thesis, KU Leuven, 2007, p.86.
[12] Dimitrov, p. 41.
[13] J. Dumortier, N. Vandezande, "Trust in the proposed EU regulation on trust services?", *Computer Law and Security Report.* nr.28 , 2012, pp. 568-576, p.571.
[14] GINI 3.2, p.20.

In particular, there are two types of risks in authentication systems: either the user is given access to a service/content he/she is not entitled to access, **or** he/she is not able to access a service/content he/she is entitled to access. This might result in damages to the SP or/and to the user:

1) The SP may suffer damage either when the SP acts in reliance on a false (or compromised) credential or assertion which it believed to be valid, or when the SP fails to rely upon a valid credential or assertion that it mistakenly believes to be false or compromised.[15]
2) The user might suffer damage when his/her personal data is misused or compromised or he/she is denied authorization to conduct a transaction he/she would normally be entitled to.[16]

These could be the result of many different failures. As an example, there could be an authentication with two FutureID Brokers (User-Broker and SP-Broker) in case of claims transformation with external IdPs, where the User-Broker derives and filters attributes and the SP-Broker acts as a validation authority for the SP and translates the assertion into a format acceptable by the SP. Several things could go wrong: the IdP could accept a false credential as authentic and provide information based on the false credential, or accept a credential but provide information which is not related to the credential; the User-Broker does not derive the right attributes or the information is sent further unfiltered (e.g. unique ID number is still in the data set) or the User-Broker could turn a response which does not provide the full information required into an adequate response by adding unverified information without indicating it; the SP-Broker could sign an assertion which is not based on the right authentication method or the new assertion does not have the same information as the original one or the SP could accept an assertion while the user is not appropriately authenticated and could give access to an unauthorized person.

This list is not exhaustive. Failures must not necessarily result in (material, or generally measurable) damage; however, if they do they can result in liability. Under certain circumstances (e.g. contractual clauses, legal obligations), there can be liability even in the absence of damages.

In the next section different sources of liability will be described and analysed.

[15] GINI 3.2, p.20.
[16] GINI 3.2, p.20.

8. Sources of liability

Liability exposure might stem from legal requirements, voluntary accepted obligations and/or general standards of diligent behaviour ('*bonus pater familias'*, see section 8.1.2).[17] We will start with non-contractual liability, since this provides the basis of the remaining types of liability. The different responsibilities and resulting liability can be extended via contracts. In several EU countries, contract law has priority over tort law.[18]

8.1 Non-contractual liability

8.1.1 Legal obligations

8.1.1.1 Data Protection Directive

The Data Protection Directive does not only provide the rights of the data subject, but also the consequences in case of noncompliance, in order to ensure that the responsible entities are incentivized to comply with the obligations.[19] Directive 95/46/EC contains a two-tiered approach: on the one hand, a pro-active approach where the responsible actors and their according obligations are identified; on the other hand, a reactive approach that, by introducing the risk of civil liability and sanctions intends to ensure that any damage caused by unlawful processing will be appropriately compensated.[20]

The obligation of the controller to ensure the data protection rights can be found in art. 23 Directive 95/46/EC, which states that persons who suffered damage as a result of unlawful processing operations or breach of national data protection legislation are entitled to compensation.[21] The provision shows that the primary responsibility for compliance is assigned to the controller.[22] The controller is the entity which decides on the why and how of the data processing.[23] If the controller has the processing carried out by a processor, the controller must choose a processor which provides sufficient guarantees

[17] GINI 3.2, p. 20.
[18] C. von Bar, U. Drobnig, *The Interaction of Contract Law and Tort and Property Law in Europe – A Comparative Study*, Sellier.European Law Publishers, München, 2004, p.189.
[19] B. van Alsenoy, "Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC", Computer law & security review 28 (2012), pp. 25-43, p. 29.
[20] B. van Alsenoy, "Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC", Computer law & security review 28 (2012), pp. 25-43, p. 29.
[21] Art. 23 (1) DPD.
[22] B. van Alsenoy, "Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC", Computer law & security review 28 (2012), pp. 25-43, p. 29.
[23] For further explanation and an overview of possible controller processor constellations, please refer to D32.8.

regarding technical and organisational security measures.[24] In this regard, the contract required by art. 17 Directive 95/46/EC assumes particular importance, since it is not the processor who is generally directly liable, but instead the controller who is liable for breaches of data protection law towards the data subject.[25] The liability of the processor would be towards the controller. In certain countries the liability of the processor can arise directly on tort grounds.[26] An example of this is the implementation of the Directive in the Dutch Data Protection Act art. 49, which provides that "processors are liable for this harm where this was incurred as a result of their actions."[27] In contrast to this provision, the liability of a data processor is not regulated under the Federal German Data Protection Act[28]. However, the data processor may be still liable according to tort law.[29] Furthermore, the data controller and the data processor are free to enter into an *inter partes* agreement on the liability of the data processor, including e.g. contractual penalties.

Art. 23 (2) Directive 95/46/EC provides that (only) if the controller is able to prove that he is not responsible for the event giving rise to the damage (e.g. in cases of fault of the data subject or in case of force majeure), he can avoid this liability wholly or partially.[30] The idea behind this is the protection of the economically weaker party, i.e. the data subject whose data is unlawfully processed.[31] This protection is realised by giving the data subject in a civil proceeding the advantage of not bearing the burden of proof that the controller has caused the damage.[32] Therefore the Directive establishes a presumption of causality which can be disproven by the controller by proving that he is not responsible for the event from which the damage results.[33] However, the Data Protection Directive has been implemented differently in each Member State, and some countries have opted not to implement art. 23 Directive 95/46/EC in this way.[34] Belgium and Portugal implemented the Directive quite verbatim, while Danish law uses more elaborate terms.[35] A similar situation exists under Federal German law. The data controller is liable for damages as far as it cannot prove that it "has exercised due care in accordance

[24] Dimitrov, p. 215.
[25] Dimitrov, p. 215.
[26] Dimitrov, p. 215.
[27] Art. 49 (3) Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens).
[28] Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 25. Februar 2015 (BGBl. I S. 162) geändert worden ist"; neugefasst durch Bek. v. 14.1.2003 I 66; zuletzt geändert durch Art. 1 G v. 25.2.2015 I 162; (BDSG).
[29] Gola/Klug/Körffer in Gola/Schomerus, Bundesdatenschutzgesetz, § 7 rec. 16 et seq.
[30] Art. 23 (2) DPD and recital 55 DPD.
[31] Dimitrov, p. 217.
[32] Dimitrov, p. 217.
[33] Dimitrov, p. 217.
[34] For example Ireland, see Dimitrov, p. 217.
[35] D. Korff, p. 180, the Danish law states that a controller is liable for "any damage caused by the processing of data in violation of the provisions of this Act unless it is established that such damage could not have been averted through the diligence and care required in connection with the processing of data".

with the circumstances of the case concerned".[36] The Dutch law provides that the level of damages can be reduced depending on the extent to which the person being sued can be held accountable for the damage, which is determined in accordance with the rules on full or partial liability.[37] Finland, France and Luxembourg apply the ordinary rules on civil and administrative liability, while in Ireland the law stipulates that controllers and processors owe a "duty of care" to the data subject, which in effect results that any breach of the law can be considered a tort. As a consequence the liability of controllers can be different, depending on which law applies to the liability issue.[38] It should be noted, however, that in the countries that follow the wording of the Directive the exemption cannot be avoided by contractual agreement, and considering the mandatory character of the provision it will probably also not be possible to agree upon a liability limitation in this regard.[39]

8.1.1.2 eSignature Directive/eIDAS Regulation

The eSignature Directive (Directive 1999/93/EC) was adopted on 13 December 1999 and entered into force in January 2000. It will be in force until 1 July 2016. It contains one provision on liability, Article 6, which states that Member States should ensure as a minimum that Certification Service Providers (CSPs) are liable for damage caused to any entity or legal or natural person who reasonably relies on certain information on a qualified certificate that has been issued or guaranteed by the CSP to the public.[40] This is, for example, that, at the time of issuance, all information contained in the qualified certificate was accurate and all the details prescribed for a qualified certificate were present, that the signatory identified in the qualified certificate held the private key corresponding to the public key in the certificate, and the assurance that the keys can be used in a complementary manner in cases where the CSP generates them both.[41] Furthermore, the CSP is liable for damage caused to a person who reasonably relies on the certificate if the CSP failed to register its revocation.[42] The CSP can evade the liability if he can prove that he has not acted negligently. Another possibility for CSPs to limit their liability is to indicate limitations to the use of the certificate, and by limiting the value of transactions for which the certificate can be used, both possible if it is ensured that the limitations are recognisable to third parties.[43] These provisions apply only to CSPs. At the current stage, the FutureID Broker is not considered to issue certificates as a CSP and therefore these provisions will generally not be applicable to

[36] § 7 BDSG. Different provisions for public bodies being a the data controller, § 8 BDSG.
[37] D. Korff, p. 180.
[38] This law might be different from the law that applies to the processing as such; D. Korff, p. 180.
[39] Dimitrov, p. 217.
[40] Art. 6 (1) Directive 1999/93/EC.
[41] Art. 6 (1) a-c Directive 1999/93/EC.
[42] Art. 6 (2) Directive 1999/93/EC.
[43] Art. 6 (3) and (4) Directive 199/93/EC.

the FutureID Broker. However, they could be applicable to CIs/IdPs, in case they would qualify as CSPs issuing qualified certificates to the public.[44]

The eIDAS Regulation[45] will repeal the e-Signature Directive. The Regulation entered into force on 17 September 2014 and its material provisions will be applicable as of 1 July 2016 (with exception to some provisions which apply earlier or later than this date). The eIDAS Regulation covers the creation/validation of electronic identities, electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services and website authentication. However, with respect to eIDs, the Regulation focuses on the mutual recognition by Member States, whereas the other services are treated as market services.[46] The Regulation is therefore divided in two sections: one on electronic identification (Chapter II) and the other one on trust services (Chapter III). Both contain liability provisions.

In Chapter III, the liability of trust service providers is described in art. 13 eIDAS. Art. 13 states that trust service providers are liable for damage caused to any natural or legal person due to failure to comply with the obligations under the Regulation. The intention or negligence of a qualified trust service provider shall be presumed unless a qualified trust service provider proves otherwise. The burden of proof regarding a non-qualified trust service provider lies with the claimant. In D33.6 the definition of a trust service provider has been detailed considering the eSign service. Similar to the eSign service, the conclusion regarding the FutureID Broker is that, considering the current description of its functionalities, these do neither constitute a trust service, nor would the FutureID Broker be a trust service provider.

In Chapter II of the Regulation, art. 11 provides strict liabilities for the notifying Member State, for the party issuing electronic identification means and the party operating the authentication procedure.[47] More specific, the party issuing the electronic identification means shall be liable for failures in ensuring that the electronic identification means is attributed to the right person in accordance with the technical specifications, standards and procedures for the relevant assurance level.[48] The party operating the authentication procedure shall be liable for damage due to a failure in ensuring the correct operation of the authentication (online possibility for the relying party to confirm the person identification data received in electronic form).[49] This only relates to cross-border transactions with notified eID means. It

[44] STORK2.0 D3.1 p. 15.
[45] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the European Union, L 257/73, 28.8.2014, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2014_257_R_0002&from=EN
[46] STORK 2.0, D3.1, p. 23.
[47] Art. 11 eIDAS.
[48] Art. 11 (3) jo. Art. 7 (e) eIDAS.
[49] Art. 11 (4) jo. Art. 7 (f) eIDAS.

becomes clear from the Regulation that the focus of its provisions is on notified national eID schemes and their use in cross-border public services. The role of the party issuing electronic identification means and the party operating the authentication procedure should be understood in this view. The role of Brokers such as the FutureID Broker is not specifically considered in this legal framework. In principle, the FutureID Broker as a legal entity in Claims Transformer Mode would be a relying party itself. The eIDAS Regulation could be applicable if the FutureID Broker would receive an assertion from a national operator of the authentication procedure, based on a notified eID. However, the Regulation provides that for relying parties other than public sector bodies the notifying Member State may define terms of access to that authentication.[50] As recognizable from the recitals, the Commission considers it beneficial if the private sector would use eID means under a notified scheme. For instance, recital 17 states that Member States should encourage private sector involvement and includes that the authentication possibility provided by any Member State should be available to private sector relying parties under the same conditions, regardless whether they are in or outside the territory of the Member State.[51] Whether or not the Member State makes their eID scheme available to private sector relying parties is left to the discretion of the Member States. However, even if the FutureID Broker would be accepted as relying party, the claims transformation and therefore the issuance of a new assertion based on the original eID would probably not fall under the scope of the Regulation.

8.1.2 Tort law

According to its recital 18, the eIDAS Regulation should provide for the liability of the Member States which notify an electronic identification means, of the party issuing it, and of the party operating the authentication procedure for failure to comply with the relevant obligations under the eIDAS Regulation. However, the express wording of the recital also provides that the Regulation should be applied in accordance with the national rules on liability. For instance, the definition of damages and the application of procedural rules including the burden of proof shall not be affected. Therefore, we will outline core aspects of European liability law, by focusing on common aspects and highlighting particularities in some Member States.

This deliverable deals with legal issues related to the FutureID component Broker Service, which is only affected by the eIDAS provisions on electronic identification and not by its material provisions on electronic signatures services. As such, the extent to which the provisions on e.g. the effect of evidence

[50] Art. 7 (f) eIDAS.
[51] Recital 17 eIDAS.

of electronic signatures[52] might impact on the law of evidence in some Member States is not to be discussed at this point.[53]

The difficulty with regard to tort law is that every country has its own concept of tort law, which has evolved over time. Even the notion of tort is not an exact term, since 'tort' is a typical common law term. 'European extra-contractual liability law excluding agency without authority and unjust enrichment' might be a more accurate description, however, it has become common to use the word 'tort' in English academic writing.[54] Due to the variations between national systems, it is difficult to provide an analysis that applies in general to all of them. Nevertheless, most systems do have some similarities. Most Member States base tort liability on the principle of fault. Fault liability refers to liability for intentional as well as negligent conduct.[55] However, nearly all systems have also some categories of tort liability that are not based on fault, usually a form of strict liability.[56] Strict liability implies that someone is liable regardless of whether he acted intentionally or negligently.[57]

The different Member States have different requirements for liability based on negligent conduct. For example, France has one requirement (faute), England two (duty of care and breach of duty) and Germany three (Tatbestand, Rechtswidrigkeit, and Verschulden).[58] However, to a certain extent they are alike, since the basic requirement for fault liability is intentional or negligent conduct. English and German law include additional requirements which mean that not every type of misconduct is sufficient for liability.[59] The interpretation of fault has evolved over time from a more subjective approach, considering the individual qualities of the tortfeasor, to a more objective one which considers the behaviour itself.[60] Therefore, nowadays, most European Member States use the objective standard, frequently presented as the famous 'bonus pater familias'. The 'bonus pater familias' is a model of an average person, "*not exceptionally gifted, careful or developed, neither underdeveloped nor someone who recklessly takes chances or who has no prudence*".[61] For some countries the concept can be adapted to the personal circumstances or time and place ('reasonable surgeon', 'careful barkeeper')[62] and for

[52] Art. 25 eIDAS
[53] Critical with regard to German civil procedure law e.g. Jandt, Beweissicherheit im elektronischen Rechtsverkehr – Folgen der europäischen Harmonisierung, NJW 2015, 1205.
[54] C. van Dam, "European Tort Law", Oxford University Press, 2013, p. 5.
[55] C. van Dam, "European Tort Law", Oxford University Press, 2013, p. 78.
[56] P. Widmer, Comparative Report on Fault as a Basis of Liability and Criterion of Imputation (Attribution), in P. Widmer (Ed.), "Unification of Tort Law: Fault", Kluwer, The Hague, 2005, p.333.
[57] C. van Dam, "European Tort Law", Oxford University Press, 2013, p. 78.
[58] C. van Dam, "European Tort Law", Oxford University Press, 2013, p.136.
[59] C. van Dam, "European Tort Law", Oxford University Press, 2013, p.136.
[60] P. Widmer (Ed.), "Unification of Tort Law: Fault", Kluwer, The Hague, 2005, p.32.
[61] P. Widmer, Comparative Report on Fault as a Basis of Liability and Criterion of Imputation (Attribution), in P. Widmer (Ed.), "Unification of Tort Law: Fault", Kluwer, The Hague, 2005, p. 348.
[62] P. Widmer, Comparative Report on Fault as a Basis of Liability and Criterion of Imputation (Attribution), in P. Widmer (Ed.), "Unification of Tort Law: Fault", Kluwer, The Hague, 2005, p. 348.

specialists generally a higher 'due care' is evaluated according to their above average capacities. The behaviour of the tortfeasor is then measured against this standard. If the behaviour does not comply with this standard and the tortfeasor did not act with due care, it is accepted that there is fault.

Further requirements for tort liability are the existence of a damage and a causal connection between the damage and the harmful behaviour.

Damage

Most Member States do not include a definition of damage in their legislation. Austria has a statutory definition (§1293 Austrian Code: "Damage is called every detriment which was inflicted on someone's property, rights or person. This is distinguished from the loss of profit which someone has to expect in the usual course of events").[63] Distinction between damage and lost profits is a technical one and today in Austria the term 'damage' is normally understood in the broad sense as the whole harm including lost profit. Even though it may start form a 'natural' meaning of damage, damage is a legal concept and only that damage which can be recovered is damage in the eyes of the law.[64] Courts and scholarly writing provide definitions in other countries, e.g. in Germany 'any loss that somebody suffered with respect to his legally protected rights, goods and interests', in Italy 'a detriment capable to be evaluated from an economic standpoint' and in the Netherlands 'factual detriment arising from a certain occurrence'.[65] All attempts agree that they presuppose a negative change (attributable to the wrongdoer) that must have taken place in the legally protected sphere of the injured party.[66] In order to judge whether a change is negative, the judge will make a comparison between two states of affairs (the so-called "Differenzhypothese" compares the situation before and after the harmful event).[67] However, the outcome depends on the positions which are included in the comparison and which worth is attributed to them. Therefore, the comparison is a method of assessing damages, but it does not in itself decide what constitutes recoverable damage.[68]

As identified in Section 7.1, the possible damage that can occur is mainly at the SP and the user side. A SP may suffer damage either when the SP acts in reliance on a false (or compromised) credential or

[63] U. Magnus, 'Comparative Report on the Law of Damages', in u. Magnus (Ed.), "Unification of tort law: damages", Principles of European Tort Law Volume 5, Kluwer, 2001, pp. 185-217, p. 190.
[64] U. Magnus, 'Comparative Report on the Law of Damages', in u. Magnus (Ed.), "Unification of tort law: damages", Principles of European Tort Law Volume 5, Kluwer, 2001, pp. 185-217, p. 190.
[65] U. Magnus, 'Comparative Report on the Law of Damages', in u. Magnus (Ed.), "Unification of tort law: damages", Principles of European Tort Law Volume 5, Kluwer, 2001, pp. 185-217, p. 191.
[66] U. Magnus, 'Comparative Report on the Law of Damages', in u. Magnus (Ed.), "Unification of tort law: damages", Principles of European Tort Law Volume 5, Kluwer, 2001, pp. 185-217, p. 191.
[67] U. Magnus, 'Comparative Report on the Law of Damages', in u. Magnus (Ed.), "Unification of tort law: damages", Principles of European Tort Law Volume 5, Kluwer, 2001, pp. 185-217, p. 191.
[68] U. Magnus, 'Comparative Report on the Law of Damages', in u. Magnus (Ed.), "Unification of tort law: damages", Principles of European Tort Law Volume 5, Kluwer, 2001, pp. 185-217, p. 191.

assertion which it believed to be valid, or when the SP fails to rely upon a valid credential or assertion that it mistakenly believes to be false or compromised.[69] A user might suffer damage when his/her personal data is misused or compromised or he/she is denied authorization to conduct a transaction he/she would normally be entitled to.[70] The scope of the damage would depend on the specific situation and would be upon the discretion of the judge.

The difficulty of assessing damage

The type of damages open for compensation might differ. Often courts are not eager to provide high compensation for immaterial damages and in general judges struggle to put a price to immaterial damages.

In Germany, in cases in which damage will only be pure pecuniary loss[71], no claim for damages may result since wealth is not protected under §823 (1) BGB. Pure pecuniary loss may, nevertheless, raise a claim for compensation under § 823 (2) BGB, but only in combination with a "protective law" ('Schutzgesetz'). "Protective law" in the German legal system is a law which is intended to protect a person; according to the legislator's incentives, such a law in its substance serves the protection of an individual against a defined type of damage.[72] For instance, when tortious behaviour leads to an unauthorised access to data, such a protective law could be § 9 of the German federal data protection law, 'Bundesdatenschutzgesetz' (BDSG). This clause requires the controller to take the necessary technical and organisational measures to ensure the implementation of the provisions of the data protection act, ensuring especially the security of the data.[73]

In the UK the data protection law in general provides for compensation for damage caused as a result of any failure on the part of a data controller to comply with the law. However, it is more restrictive with respect to "distress" (immaterial damage) than with respect to (material) damage, as distress can only be awarded if material damage has been proven.[74] In such respect, the UK ruling is very interesting to demonstrate that over time countries can become more open to the possibility of awarding immaterial damage. A recent court case in the UK changes the current understanding of damage in the UK data protection act.[75] The court ruled that misuse of private information is a tort. The judges concluded that article 23 Directive 95/46/EC has a wide meaning, including both material and non-material damage, establishing that the definition of damage in the UK act is not in line with the European Data Protection Directive 95/46/EC.

---

[69] GINI 3.2, p.20.
[70] GINI 3.2, p.20.
[71] In German 'Vermögensschaden', it means pure financial damage, not any damage to persons or goods.
[72] BGH Urteil VI ZR 33/81 29.6.1982.
[73] G. Borges, Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis - Ein Gutachten für das Bundesministerium des Innern, 2010, p.199, available at: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/PaesseAusweise/rechtsfragen_npa.html
[74] Korff, p.180.
[75] Vidal-Hall & Ors v Google, EWCA Civ 311 Court of Appeal 2015.

This example shows that with regard to the scope of damage in respect to data, no final understanding has been reached so far. It remains an ongoing discussion in how far immaterial damage shall be restituted, and how it should be assessed.

Causation

In order to establish liability for a damage, a connection between the liable person and the damage needs to exist. Most legal systems consider *conditio sine qua non* as a first test for causation. Only in Belgium *conditio sine qua non* is the sole requirement to be established and Belgium officially rejects the two step approach which other jurisdictions take as a theoretical framework.[76] *Conditio sine qua non* requires the judge to determine whether an act or omission was a cause of the rights violation. This is done by considering whether the loss would still appear if the act or omission was eliminated. If the loss does not occur, the act or omission was not causal for the loss, if it does, the loss has been caused by the act or omission.[77] The second step can be different in the different legal systems. Common law considers the 'proximate cause', which includes proximity in time and space, foreseeability of the harm and other factors.[78] Other countries such as France, Germany, Greece and Austria use the test of adequate causation.[79] In this regard the degree of probability is decisive. For example, in Austria, adequacy is established if the damaging event was to a considerable extent generally suitable for increasing the possibility of such a damage as in fact occurred.[80]

As it is recognizable from the analysis, tort law varies in the different countries and therefore the scope of liability of the FutureID Broker generally depends on the applicable law, the exact tort and the discretion of the judge. As a general guideline, the FutureID Broker should ensure to comply with all applicable norms and standards and act with due care. In this regard it is useful for the FutureID Broker to log events, in order to be able to prove e.g. that systems were working according to the standards, and that no fault occurred at the Broker side.

8.1.3 Conclusion non-contractual liability

In this section we analysed the non-contractual liability that might be relevant to the FutureID Broker. The analysis was done considering Data Protection law, e-signature/eIDAS legislation and tort law. It becomes clear that for non-contractual liability tort law plays an important role. Data protection

[76] J. Spier and O. A. Haazen, "Comparative Conclusions on Causation", in J. Spier (Ed.): Unification of Tort Law: Causation, Kluwer, 2000, p.127.
[77] J. Spier and O. A Haazen, "Comparative Conclusions on Causation", in J. Spier (Ed.): Unification of Tort Law: Causation, Kluwer, 2000, p.127.
[78] J. Spier and O. A Haazen, "Comparative Conclusions on Causation", in J. Spier (Ed.): Unification of Tort Law: Causation, Kluwer, 2000, p.130.
[79] J. Spier and O. A Haazen, "Comparative Conclusions on Causation", in J. Spier (Ed.): Unification of Tort Law: Causation, Kluwer, 2000, p.132.
[80] J. Spier and O. A Haazen, "Comparative Conclusions on Causation", in J. Spier (Ed.): Unification of Tort Law: Causation, Kluwer, 2000, p.132.

obligations are often implemented in the national legislation that they are enforced via tort law. For data protection law, the practical division between controller and processor remains important. If the FutureID Broker is a controller, it will be the main responsible party which has to comply with the data protection obligations. In case of non-conformance, this can result in a higher liability risk. If the FutureID Broker is a processor, there are less obligations, but the Broker might still face liability claims. These might either be from the data subject on the basis of tort law, or the controller might hold the processor liable on the basis of contractual clauses in the controller-processor contract.

The legislation on electronic signatures changed and was broadened under the eIDAS Regulation, covering also other trust services and notified identity services. In this regard, the risk of liability is lower for the FutureID Broker, as with its current service profile it does not qualify as a certification service provider/trust service provider in the sense of the legislation. The eIDAS Regulation provides liability for the party issuing the electronic identification means, the party operating the authentication procedure and the notifying Member State. However, the focus of the Regulation is on notified national eID schemes and their use in cross-border public services. The role of Brokers such as the FutureID Broker is not specifically considered in this legal framework. In principle, the FutureID Broker as a legal entity in Claims Transformer Mode could be a relying party itself. The eIDAS Regulation could be applicable if the FutureID Broker would receive an assertion from a national operator of the authentication procedure, based on a notified eID, giving the FutureID Broker some rights vis-à-vis the named parties. Nevertheless it has to be taken into account that the rules are intended for public services and the Regulation leaves the choice to accept private relying parties to the Member States, including the possibility to define terms of access, which could entail liability limitations.

Finally, tort law is the general redress system. It varies substantially between Member States, but usually requires a fault, a damage and a causal connection between the fault and the damage. It will often be difficult for the user and the SP to demonstrate that they suffered a material damage. Non-material damage can be awarded, but the judges are often more reluctant in this regard. Taking into account the heightened importance of data, this might change in the future. The characterisation of the fault is another difficulty, as it is not yet defined which rights and obligations the FutureID Broker has.[81] These might result from contracts under which the failure to comply with contractual obligations might not only give rise to pre-defined contractual liability, but also to tort liability.

8.2 Contractual liability

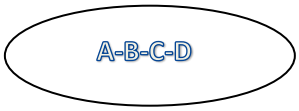
The technical components built in the FutureID project can be implemented in different ways. The idea of the FutureID project is that no centralized infrastructure exists, but instead it will be an ecosystem with free participation of an open number of stakeholders. Therefore, most likely a decentralized

[81] see also STORK D3.1, p.36.

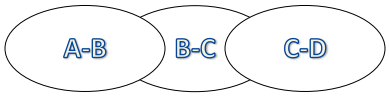
governance structure will exist. This requires a certain amount of trust that the stakeholders need to place in each other. By itself, non-contractual liability might not be enough to foster this trust. Therefore, contractual liability might be an important trust enabler. In general, the interaction between the different actors will most likely be subject to a contractual network.

Contractual networks can take at least four different legal forms:[82]

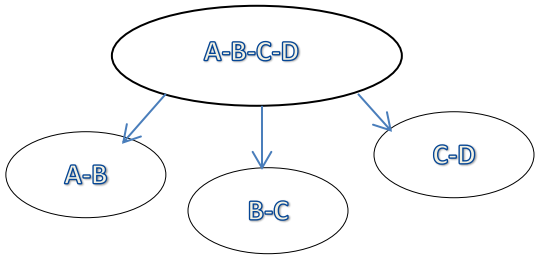
- a multilateral contract (three or more parties agree to coordinate complex economic operations, typical examples being the contract of consortium): contract between A, B, C and D, each party undertakes obligations towards each party of the contract in order to achieve a common goal.[83]



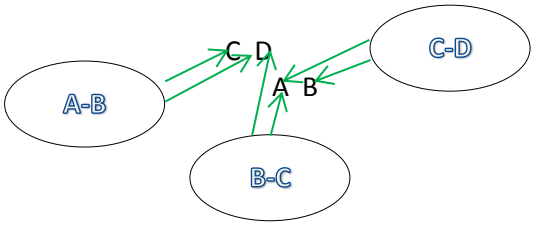
- a set of interdependent "linked" bilateral contracts



- an intermediate form consisting of a multilateral contract as a framework contract and bilateral executory contracts between parties to regulate the specific elements of the transaction;



- contracts for the benefit of a third party: A-B conclude a contract for the benefit of C and D, B-C one for A and D, etc.



[82] see F. Cafaggi, 'Contractual Networks and the Small Business Act', EUI WP Law 2008/15, p. 12ff.
[83] F. Cafaggi, 'Contractual Networks and the Small Business Act', EUI WP Law 2008/15, p. 16.

8.2.1 Contractual relationships

The decentralized governance structure would require that every actor enters into contracts with the other participants they want to work with/rely upon. The exact configuration of the contractual framework cannot be foreseen at this point, but presumably it will include at least these relationships.

The user will normally have a (contractual) relationship with the CI/IdP and the SP. These relationships fall outside of the scope of FutureID. The user could furthermore have a contractual relationship with a FutureID Broker, which will be called the User-Broker here. This relationship will most likely be governed either by an individual (consumer) contract or by the terms and conditions set by the User-Broker, which the user needs to accept. This is a business to consumer (B2C) relation.

We assume that the SP typically will have a contractual relationship with a FutureID Broker (SP-Broker) with which it has direct contact. This contractual relationship, among others, will ensure that only trusted credentials and intermediaries are used. Depending on the status of the FutureID Broker as controller or processor, the contract must include the relevant data protection clauses.

User-Broker and SP-Broker can be a single legal entity, but can also be separate ones. Therefore, the FutureID Brokers can have contractual relationships with other FutureID Brokers. This could even result in a chain of different FutureID Brokers, all connected via contracts. Additionally, it needs to be assessed which actor is controller and which processor, and the contracts be drafted accordingly.

Furthermore, it might be necessary that every FutureID Broker enters into contracts with the CIs/IdPs whose authentication services (remote verification of the credential and issuing of a signed assertion) the Broker uses. Especially in the beginning, when the FutureID Broker has a low bargaining position, this could often entail that the FutureID Broker will need to adhere to obligations set by the CIs/IdPs, since those often have a stronger market position. In this regard it is important to note that Art. 7(f) eIDAS provides that “for relying parties other than public sector bodies the notifying Member State may define terms of access to that authentication.” This might often preclude any bargaining possibilities. From a technological point of view, the communication between the FutureID Broker and CIs/IdPs is not direct. However, most current assertion technologies require that a Broker is explicitly listed in the assertion as intended recipient, which gives the possibility to the IdP to provide service only for selected Brokers and also to bill Brokers for rendered services.[84]

With the exception of the contract entered with the user, all the remaining relationships would normally be business to business (B2B) relationships. Generally, the contents of B2B contracts can be freely decided by the contracting parties, since the principle of freedom of contract applies without legal

[84] Expert information.

restrictions stemming from consumer protection legislation. However, for practical reasons, some topics should be addressed in the contracts:[85]

- Role and responsibilities of each of the stakeholders
- Agreements on applicable law and dispute resolution
- Data protection compliance requirements
- Possibly: Obligation to implement and follow inputs and instruction from the Governing Entity (including e.g. use of current code and update requirements, security requirements)
- Possibly: Service Level Agreements
- Liabilities that they accept towards each stakeholder, including financial limitations, possibly linked to applicable Levels of Assurance (LoAs).

8.2.2 Liability and possible factors

In theory, a wide range of liability models is possible. The SP could rely on an eID solution without any ability of recourse even if the FutureID Broker/IdP does not act in accordance with its stated practices; a capped liability is possible where the FutureID Broker/IdP might agree to indemnify SPs to a certain amount; an objective liability of the FutureID Broker/IdP might be installed; there might be a pooled liability scheme jointly funded by the participants of the FutureID system, etc.[86]

Levels of Assurance (LoA)

LoAs are used in identity management systems to indicate the degree of confidence. They should "*characterise the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned*".[87] Different definitions and systems of assurance levels exist, resulting from projects such as the STORK project, and different standardisation activities[88].

Across the different LoAs, the introduction of the eIDAS Regulation might be positive. Art. 8 of the eIDAS Regulation describes three levels: low, substantial and high. LoA 'low' indicates identification means which only provide a limited degree of confidence, and the specifications, standards, procedures and

[85] based on STORK D3.1, p. 36f.
[86] GINI 3.2, p.20.
[87] eIDAS Regulation, recital 16.
[88] e.g. STORK Quality Authentication Assurance (QAA) model (Described in STORK D2.3, Quality authenticator scheme, https://www.eid-stork.eu/index.php?option=com_processes&act=list_documents&s=1&Itemid=60&id=312), ISO 29115, ITU-T Recommendation X.1254 (https://www.itu.int/rec/T-REC-X.1254-201305-I!Err1/en).

controls have the purpose to decrease the risk of misuse or alteration of the identity.[89] 'Substantial' refers to identification means which provide a substantial degree of confidence, and the specifications, standards and procedures intent to decrease substantially the risk of misuse or alteration of the identity.[90] The LoA 'high' finally refers to identification means which provide a higher degree of confidence than identification means with the LoA 'substantial', and the purpose of the technical specifications, standard, procedures and technical controls is to prevent misuse or alteration of the identity.[91] The Commission issued an Implementing Regulation on assurance levels.[92] The Implementing Regulation sets specifications and procedures in its Annex for determining the three different levels. This is done by considering not only the reliability and quality of the enrolment but also the electronic identification means management and the authentication itself.[93] Furthermore, the general management and organisation of participants which provide a service related to electronic identification in a cross-border context is considered in assessing the assurance level.[94] Based upon this, the assurance levels of electronic identification means can be determined. Considering that the requirements are supposed to be technology neutral, it should be possible to achieve them with different technologies.[95]

When notifying an authentication means to the Commission according to art. 9 eIDAS, the notifying Member State has to indicate the LoA of the identification means, and the national assurance levels of notified national eID means shall be mapped against the eIDAS LoAs in the interoperability framework.[96] This indicates that the eIDAS assurance levels can become the generally accepted standards, which would make it easier to refer to them in contracts.

In the FutureID contracts, the LoAs of the different electronic authentication means could be used to indicate different levels of accepted liability. For example, in a case where the eID means have no level of assurance or only a low level, it could be accepted that no recourse is possible. Differently, in cases of high assurance levels, the Broker/IdP might agree a stricter liability.

Other factors

[89] art. 8 (2) (a) eIDAS.
[90] art. 8 (2) (b) eIDAS.
[91] art. 8 (2) (c) eIDAS.
[92] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8 (3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
[93] art. 1 (2) Commission Implementing Regulation (EU) 2015/1502.
[94] art. 1 (2) Commission Implementing Regulation (EU) 2015/1502.
[95] Recital 16 eIDAS Regulation, specifications in the Annex of Commission Implementing Regulation (EU) 2015/1502.
[96] art. 12 (4) (b) eIDAS.

At this point in time, it is not yet possible to determine the control level of each stakeholder. However, this can be of significance to assess the corresponding (potential) liability.[97] An increased level of control will normally relate to an increased risk of liability. However, this might deter participants from taking more responsibilities within the FutureID Ecosystem. Therefore, in the contractual negotiations for a credible solution, it will be necessary to find a way of appropriately associating risk with responsibility without precluding the potential of participation as a result.[98] The possibility of obtaining insurance coverage against certain liability risks could assume relevance. Another influencing factor could be the bargaining position of the stakeholders, as indicated in 8.2.1.

8.2.2.1 Governing entity

The choice between the possible contractual frameworks will depend on the different stakeholders. However, if the different stakeholders intend to work under a single trade mark or distinctive sign (e.g. "FutureID"), any misbehaviour of one stakeholder might result in detrimental consequences and general loss of trust for every participant. In this case it can be advisable to have a governing authority, which sets standards, provides code and supervises the adherence to the rules. This governing authority could also provide some general terms (especially regarding liability) that need to be obeyed, which could balance otherwise possibly existing imbalances in bargaining powers.

8.2.2.2 Liability in contractual chains

Where the participants in the ecosystem enter into bilateral contracts with other participants they have a direct relation with, but not with previous participants (e.g. the SP will have a contract with the FutureID Broker, but not with the IdP on whose assertion the SP will basically rely upon), a contractual chain is established. In this contractual chain the trust needs to be ensured. This can be done via liability.

The principle that a contract can only confer rights and impose obligations to the contracting parties is known in civil countries as "relativity of contract". In common law systems, it is termed "privity of contract".[99] The doctrine of privity/relativity entails two prohibitions: (1) contractual duties cannot be imposed on an unconsenting third party, (2) third parties cannot acquire rights under a contract to which they are not a party.[100] In most European legal orders, to prevent contract law from "drowning in a sea of torts", the principle of privity (or relativity) of contract is flanked in tort law by the principle that a

[97] TAS^3, D6.1-2, p. 105.
[98] TAS^3, D6.1-2, p. 105.
[99] M. Ebers, A. Janssen, O. Meyer (ed), European Perspectives on Producers' Liability, sellier.european law publishers, 2009, p. 7.
[100] M. Ebers, A. Janssen, O. Meyer (ed), European Perspectives on Producers' Liability, sellier.european law publishers, 2009, p.7.

pure economic loss is only eligible for compensation under very specific circumstances. This ensures that tort cannot be used to indirectly expand the sphere of contractual obligations.[101]

An example of this can be seen in the sale of goods. Goods are usually supplied along a distribution chain, starting with the producer, continuing with the importer, the wholesaler, the final seller and lastly the consumer.[102] Similar to what is foreseen to occur with FutureID, the contractual relations in the distribution chain are often done via a number of individual, bilateral contracts.[103] The European Consumer Sales Directive (Directive 1999/44/EC) harmonises the rights and remedies available to consumers where the goods sold do not conform to the contract.[104] The one liable to the consumer for any non-conformity is the final seller of the consumer goods.[105] However, art. 4 of the Directive provides the final seller with a right of redress:

> "*Where the final seller is liable to the consumer because of a lack of conformity resulting from an act or omission by the producer, a previous seller in the same chain of contracts or any other intermediary, the final seller shall be entitled to pursue remedies against the person or persons liable in the contractual chain. The person or persons liable against whom the final seller may pursue remedies, together with the relevant actions and conditions of exercise, shall be determined by national law.*"

However, in most countries this claim of redress can only be brought against the supplier, which would then have a claim against his contractual partner and so on, until the liability reaches the responsible party.[106]

Differently from the sale of consumer goods, no European laws (except for the eIDAs Regulation, which only covers the liability in case of notified eID schemes for public services) specifically regulate the liability within (federated/user-centric) identity management contractual chains. However, the doctrine of privity/relativity entails that any claim for redress can only be against the other party of the contract. Therefore back-to-back liability arrangements can be useful in FutureID. The approach of contractual

[101] M. Ebers, A. Janssen, O. Meyer (ed), European Perspectives on Producers' Liability, sellier.european law publishers, 2009, p.7.
[102] M. Ebers, A. Janssen, O. Meyer (ed), European Perspectives on Producers' Liability, sellier.european law publishers, 2009, p. 3.
[103] M. Ebers, A. Janssen, O. Meyer (ed), European Perspectives on Producers' Liability, sellier.european law publishers, 2009, p. 3.
[104] M. Ebers, A. Janssen, O. Meyer (ed), European Perspectives on Producers' Liability, sellier.european law publishers, 2009, p. 3.
[105] M. Ebers, A. Janssen, O. Meyer (ed), European Perspectives on Producers' Liability, sellier.european law publishers, 2009, p. 3.
[106] M. Ebers, A. Janssen, O. Meyer (ed), European Perspectives on Producers' Liability, sellier.european law publishers, 2009, p.3.

(liability) chains is especially interesting with respect to a privacy-friendly implementation of the FutureID infrastructure. This is explained in more detail in D12.9.

8.2.3 Conclusion contractual liability

The reference architecture allows the components to be implemented in different ways. In general it envisages a strongly decentralized deployment. This would entail that every participant of the FutureID ecosystem would enter into contracts with the party they rely upon. As explained, this will normally result in a chain of contracts. As such, it is important that the FutureID Broker enters into back-to-back liability arrangements to ensure that there is no gap in contract coverage that would leave the Broker with uncovered risks. If the FutureID Broker has to take on certain responsibilities that cannot be covered in contracts for example with the IdP, it might be an option to take an insurance to reduce the risk. In order to have a stable system, and particularly where a single trade mark or distinctive sign is used, a governing entity should establish and (possibly) enforce the obligations of the different participants. Participating parties should consider in their contracts the role and responsibilities of each partner. Furthermore, they should agree on applicable law and dispute resolution and which liabilities are accepted towards each stakeholder (including financial limitations). They should additionally enter into Service Level Agreements and provide for obligations to implement and follow inputs and instructions from the governing entity. Finally they should also cover the data protection requirements, possibly by means of controller-processor contracts.

8.3 Liability exemption

This final subsection will analyse whether the FutureID Broker might be able to make use of the liability exemptions provided by Directive 2000/31/EC.[107]

The FutureID Broker acts as an intermediary in the authentication process. It is likely that the FutureID Broker will provide its service for some kind of remuneration. Furthermore, the service will be provided at a distance, by means of electronic equipment, and at the individual request of a recipient of the service. Therefore, the FutureID Broker will provide an information society service under art. 2 (a) Directive 2000/31/EC. None of the exclusion of application under art. 1(5) Directive 2000/31/EC apply and, therefore, the FutureID Broker shall be subject to the provisions of Directive 2000/31/EC. This section analyses whether the FutureID Broker is eligible for the liability exemptions provided in this legal instrument.

Directive 2000/31/EC provides three liability exemptions for intermediaries: mere conduit, caching and hosting. Mere conduit aims at transmission services (information goes from computer to computer) and

[107] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

access services.[108] Transmission means a transfer of information from computer to computer.[109] This information will be stored on any of the computers for a short moment of time.[110] This temporal storage can be considered part of a "transmission" if the storage is automatic (by machines, not humans), intermediate (in the course of a transmission) and transient (for a limited period of time).[111] The storage needs to be made for the single purpose of facilitation of the transmission, and the information may not be stored any longer than is reasonably necessary for this goal.[112] For the exemption to apply, the SP needs to fulfil certain requirements. The SP must ensure that it did not initiate the transfer of data, nor select the recipients of the data, nor modify the transmitted data.[113] As recognizable from this, the exemption only applies "where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network".[114] The information society service provider may in no way be involved with the transmitted information, and the only allowed way of modification of the information is manipulation of a technical nature in the course of transmission, which does not alter the integrity of the information contained.[115] However, where the legal system of a Member State provides for it, it is still possible for a court or administrative authority to order the SP to terminate or take measures to prevent a particular infringement.[116] It is possible that the FutureID Broker in the dispatcher mode might fall under this exemption, if it only routes the information to the SP, but is in no way involved in any decision or changes to the content.

The other two exemptions are caching and hosting, which both apply to storage of information. Caching is "*the automatic, intermediate and temporary storage of […] information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request*".[117] Hosting can be described as the storage of information which has been provided by the recipient of the service. The information society service provider shall not be liable for the information which is stored at the request of a recipient of the service, if it does not have actual knowledge of illegal activity or information. It is unlikely that these exceptions could apply to the FutureID Broker in any of the modes, as it will not store the information, neither to make it faster accessible nor to host it for the user or SP.

In general, the Member States can impose two obligations on information society service providers, regardless whether they meet the exemptions or not: they can oblige them to inform the authorities of

[108] GINI 3.1, p. 62.
[109] Lodder , p. 87.
[110] Lodder, p. 87.
[111] Lodder, p. 87.
[112] Art. 12 (2) Directive 2000/31/EC .
[113] Art. 12 (1) Directive 2000/31/EC .
[114] Recital (42) Directive 2000/31/EC .
[115] Recital (43) Directive 2000/31/EC .
[116] Art. 12 (3) Directive 2000/31/EC .
[117] Art. 13 (1) Directive 2000/31/EC .

illegal activities/information, as soon as the information society service provider becomes aware of them, and to disclose the identity of recipients with whom they have storage agreements.[118]

The noncompliance with these requirements does not result in liability per se. It only means that the information society service provider cannot make use of the exemptions.

[118] Art. 15 (2) Directive 2000/31/EC .

9. Dutch case-study

In the Netherlands, there have been two important cases demonstrating the vulnerability of eID schemes. The first relates to the DigiD system and was caused by a system of authorisations that turned out to be susceptible to fraud. The second example is the Diginotar case, where a Dutch certification provider was compromised by a hack.

The DigiD system allowed third parties to manage government affairs on behalf of interested parties. The so-called DigiD Machtigen (DigiD Authorisation) turned out to be susceptible to abuse as it did not provide adequate guarantees. Instead, it easily allowed to amend the personal information of the DigiD holder, including bank account information. This allowed benefits to be wired to a third party account, having the DigiD holder deprived of those benefits. Malicious third parties convinced DigiD holders that they were kind enough to "help" them fill out their benefit forms, while in fact they amended the personal data of the DigiD holder, redirecting the benefits to their own account.

In another large scale fraud case with DigiD, personal information of over 50 Dutch students was stolen, most probably by simply getting the DigiD confirmation letters with activation codes from the students' mailboxes. By changing students' information, users were locked out of their own accounts and their money and other benefits were rerouted to different accounts.

The liability of the malicious third parties is of limited relevance to the present analysis. It is enough to mention that the cases were resolved and that the system for authorizations has been changed to prevent fraud. The relevance of the example to FutureID lays in the (potential) accountability of DigiD.

There were no Dutch court cases against the ministry responsible for DigiD or the tax authorities that relied on DigiD. So the authorities were not held accountable for the problems. In fact, a lower Dutch administrative court ruled that the Ministry of Economic and the tax authorities are not responsible for the fraud or its consequences. On the contrary, the Dutch tax authorities have tried to claim money back from DigiD holders with whose DigiD benefits had been claimed that turned out to be fraudulent. The Dutch highest administrative court, The Council of State (Raad van State), ruled that in principle the holder of a DigiD was responsible for the DigiD and its correct use, and thus for keeping it confidential and free from abuse. However, in this specific case, the court stated that: "The case revealed that it has been possible, during a very limited period in 2010, to file a DigiD request in name of someone else. As the tax authority was unable to prove whether the DigiD holder herself, or a malicious third party in her name, has requested and used the DigiD without knowledge of the defendant, the defendant is not responsible to pay back the benefits the tax authority provided".

The second case, Diginotar, was about a compromised Dutch certificate authority. In order to conduct trusted business online, websites require certificates. These are used to prove the identity of the web site operator and are known as SSL certificates. For transactions with the government (e.g. the Dutch tax authority and the use of DigiD) other certificates – Public Key Infrastructure (PKI) certificates – are used.

If a certificate gets compromised, so-called 'man-in-the-middle' attacks (MITM)[119] can take place. In the Dutch DigiNotar case, the system was hacked, leading to fraudulent certificates. It soon became clear that not only the Internet certificates, but also the government certificates were at issue. Government stepped in, DigiNotar went bankrupt and a process of transition to other PKI certificate suppliers was put in motion.

Under the Dutch Telecommunications Act (Telecommunicatiewet), the Dutch Telecommunication authority is charged with supervising 'qualified certificates' (also called 'digital signatures'). The PKI certificates at issue belong to these regulated certificates in need of registration with the Dutch Telecommunications Authority, for which the Authority can also decide to withdraw the registration. This happened with DigiNotar, which was forced to withdraw the qualified certificates that had been issued within 14 days.

In respect of liability, the Dutch Civil Code contains article 6:196b BW, but the same only applies to qualified certificates. The normal liability regime of breach of contract and unlawful act is applicable to other certificates. Since the SSL-certificates of DigiNotar were not qualified certificates, 6:196b BW did not apply.

Instead, the issue would be one of contractual liability. DigiNotar has a contractual obligation to its customers to deliver well-functioning SSL-certificates. If DigiNotar stops fulfilling its obligation, there is a breach of contract and a claim for damages can be filed (art. 6:74 of the Dutch Civil Code). However, the success of such a claim is not clear as, under the applicable general terms and conditions, there was a limitation of DigiNotar's liability. As Diginotar claims its certificates to be trustworthy (and this turned out not to be the case), a claim for damages can also be based on this incorrect statement, opening the possibility for a claim on the basis of unlawful conduct (art. 6:162 of the Dutch Civil Code).

These national cases show that authentication systems are complex, many parties are involved, and it is difficult to prove what exactly caused the failure. In general the approach seems to be that the authentication means and the system are deemed secure, and if something goes wrong it is expected that it has been the fault of the user (see the example of DigiD). Therefore in practice the risk for other parties to be held liable seems rather small. The case of Diginotar shows that, as far as is known, Diginotar was not held liable by users. However, the example shows very well that losing the trust of the users can have detrimental economic consequences, in this case bankruptcy. For FutureID this shows that even though the liability risk of the FutureID Broker might in praxis at the moment not be very high, the loss of trust could form an even higher risk than possible liability claims.

[119] An attack where two parties believe they are directly communicating with each other, but an attacker secretly relays and possibly alters the communication between them.

10. Conclusion

This deliverable aimed to provide an analysis of the legal framework surrounding the FutureID Broker with a special focus on liability.

With this purpose, it starts with an introduction to the functioning of the FutureID Broker and the FutureID Ecosystem. This was followed by information on the importance of liability within the identity management context as an enabler of trust by providing a high-level conceptualization of the various expectations held by the different entities that participate in FutureID. The main part of this deliverable provides an overview of the different sources of liability and how they could apply to the FutureID Broker. This starts with an overview of non-contractual liability by considering Data Protection law, e-signature/eIDAS legislation and tort law. It becomes clear that tort law plays an important role for non-contractual liability. For data protection law, the distinction between controller and processor remains important, as if the FutureID Broker is a controller, it will be subject to more stringent obligations and, hence, a higher risk for liability. On the other hand, if the FutureID Broker is simply a processor, it shall be subject to less onerous obligations, although it might still face liability claims. Depending on the national implementation of the data protection law, the FutureID Broker might be held directly liable as a processor, or via contractual clauses in the controller-processor contract by the controller/SP.

The legislation on electronic signatures changed, and was broadened under the eIDAS Regulation. It covers now other trust services and notified identity services. The FutureID Broker will most likely not have to face liability under the e-signature Directive or eIDAS Regulation, as with its current service profile it does not qualify as a certification service provider/trust service provider in the sense of the legislation. The role of Brokers such as the FutureID Broker is not specifically considered under the eIDAS Regulation. In principle, the FutureID Broker as a legal entity in Claims Transformer Mode would be a relying party. If the FutureID Broker would receive an assertion from a national operator of the authentication procedure, based on a notified eID, the eIDAS provision might give the FutureID Broker some rights vis-à-vis the party issuing the electronic identification means, the party operating the authentication procedure or the notifying Member State. Nevertheless it has to be taken into account that the rules are aimed at public services and that the Regulation leaves the choice to accept private relying parties to the Member States, including the possibility to define terms of access, which could entail liability limitations. Finally, tort law varies substantially between Member States, but usually requires a fault, a damage and a causal connection between the fault and the damage. It will often be difficult for the user and the SP to demonstrate that they suffered a material damage. Non-material damage can be awarded, but the judges are often more reluctant in this regard. Taking into account the heightened importance of data, this might change in the future. The characterisation of the fault is another difficulty, as it is not yet defined which rights and obligations the FutureID Broker has. These might result from contracts, under which the failure to comply with contractual obligations might not only give rise to pre-defined contractual liability, but also to tort liability.

The contractual liability will depend on the exact provisions in the contracts. The reference architecture allows the components to be implemented in different ways. In general it envisages a strongly decentralized deployment. This would entail that every participant of the FutureID ecosystem would enter into contracts with the party they rely upon. As explained, this will result in a chain of contracts. As such, it is important that the FutureID Broker enters into back-to-back liability arrangements to ensure that there is no gap in liability coverage that would leave the Broker with uncovered risks. In particular when a single trade mark or distinctive sign would be used, it might be advisable that a governing entity would establish and (possibly) enforce obligations for the different participants. Points which should be considered in the contracts are the role and responsibilities of each partner, the applicable law and dispute resolution and which liabilities are accepted towards each stakeholder (including financial limitations). The contracting partners should also consider Service Level Agreements and provide for obligations to implement and follow inputs and instructions from the governing entity. Finally they should also cover the data protection requirements, possibly by means of controller-processor contracts.

To complete the analysis, the position of the FutureID Broker under the Directive 2000/31/EC was assessed. The provisions of this Directive seem to apply as the FutureID Broker will provide an information society service. However, it does not seem likely that the FutureID Broker can benefit from the liability exemptions. An exception might be the Broker in Dispatcher Mode, who might be able to invoke the exemption of mere conduit (this is however disputable). As the FutureID Broker will not provide a hosting service, it is clear that the exemptions of caching and hosting are not applicable.

Finally the analysis concludes with examples of failures in authentication systems in the Netherlands. These examples show that the risk of liability claims is currently reduced and can be countered with limited liability clauses. However, a bigger risk is the loss of trust, which can finally result in bankruptcy.

Therefore, it is advisable that the FutureID Broker establishes adequate liability limitations and back-to-back liability arrangement, while at the same time ensuring the trust between all the parties. This could include the provision of simple redress mechanisms and support and contact points. This would allow users to have support when problems arise and avoid them to be forced to prove what went wrong in a system they do not understand. Finally, logging is advisable, as it can provide evidence in the question whose fault the failure was, and therefore facilitate getting redress from the liable party.