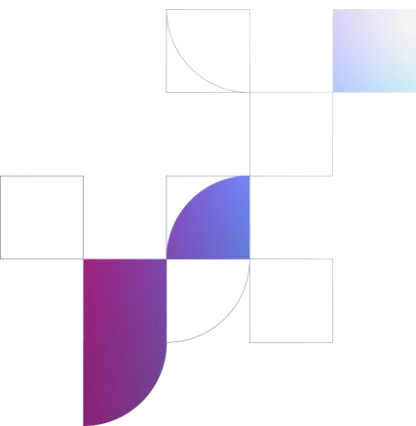


BEREC report on interoperability of Number-Independent Interpersonal Communication Services (NI-ICS)



December, 2022

Contents

Executive Summary.....	2
1. Introduction	4
2. NI-ICS and scope of the report.....	6
2.1. Definition.....	6
2.2. Categories.....	6
2.3. Scope of the report	9
3. Economic and behavioural features of messaging services	9
4. The state of the market for messaging services	12
4.1. Main applications/actors.....	12
4.2. Use of messaging services	13
4.3. Multi-homing.....	14
5. Interoperability measures	15
5.1. Objectives and types of interoperability measures.....	15
5.2. Interoperability approaches	17
5.2.1. Technical solutions.....	18
5.2.2. Standardisation	20
5.3. Implementation challenges.....	21
5.3.1. Specifying the interoperability approach and interoperable functions.....	22
5.3.2. Ensuring innovation in an interoperable environment	22
5.3.3. Ensuring a high level of data protection and security	23
5.4. Summary of findings.....	26
6. Interoperability of NI-ICS under the DMA	28
6.1. Definition of core platform services and designation of gatekeepers	29
6.2. Interoperability of NI-ICS under the DMA.....	29
6.3. Technical implementation	31
6.4. Governance.....	33
7. Interoperability of NI-ICS under the EECC.....	33
7.1. NI-ICS in the ECS regulatory framework.....	33
7.2. Article 61(2) EECC	36
7.2.1. Procedure for imposing interoperability on NI-ICS	36
7.2.2. Conditions for imposing interoperability on NI-ICS	38
8. Interplay between the DMA and the EECC	42
9. Conclusions.....	45
10. Future work.....	46
ANNEX 1: List of abbreviations	48
ANNEX 2: List of figures and tables	49

Executive Summary

Number-Independent Interpersonal Communication Services (NI-ICS) are interpersonal communication services which do not connect with publicly assigned numbering resources, or which do not enable communication with a number in national or international numbering plans. NI-ICS typically include messaging, video-conferencing and e-mail services. The use of NI-ICS has drastically increased in the last decade and such services have now become a crucial means of communication for a variety of different users throughout Europe.

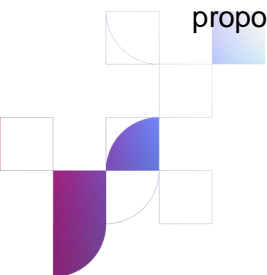
Most NI-ICS exhibit very strong proprietary network effects, as users can typically communicate only with other users of the same service. Although multi-homing is possible and common, the market for messaging services appears to be significantly concentrated around very few players. In order to unleash and share such network effects among several providers, and thus facilitate market contestability, interoperability obligations for specific NI-ICS providers are included under Article 7 of the Digital Markets Act (DMA) and, with a focus on ensuring end-to-end connectivity, under Article 61(2) of the European Electronic Communications Code (EECC).

Interoperability is the ability of two or more systems or components to exchange information and to use the information that has been exchanged. To this end, it requires a common understanding among players on several aspects, and can be implemented via e.g. interfaces set by the provider or a standardisation process. Interoperability is not an end in itself, but a means to reach specific objectives. It can do so by following different approaches and technical implementation options.

After presenting the main economic features and the state of the market for some NI-ICS, BEREC explores and analyses i) the objectives, the scope and the “triggers” of interoperability obligations under both the DMA and the EECC, ii) the potential technical approaches and the implementation challenges to be taken into account when applying these measures, as well as iii) the interplay between the two regulatory frameworks (DMA & EECC). The current work focuses on messaging services, but other NI-ICS may be further analysed by BEREC in the future.

BEREC supports the asymmetric regulatory approach chosen under both the DMA and the EECC. Only gatekeepers (designated under the DMA) and key providers with a significant level of coverage and user uptake (designated under the EECC) shall make their services interoperable, under the conditions detailed in the respective legislations. Providers which do not fall within these categories will have the choice to interoperate (or not) with them.

In this context, different technical implementation options and procedures are possible: private actors may develop and give access to their own technical solutions such as application programming interfaces (APIs) or bridges, or the solutions can be developed through formal standardisation. Such options have advantages and disadvantages that need to be considered and balanced when applying interoperability measures. For instance, APIs proposed/designed by the NI-ICS gatekeeper/key provider can allow for more dynamic and



rapid changes, but interfaces are usually provider-specific and therefore likely to differ from one another. On the other hand, standards are often defined in a context including several stakeholders, but the process can be lengthy and, sometimes, inefficient. Regardless of the chosen approach, BEREC believes that it is crucial to include an appropriate updating mechanism, allowing for adding new functions, quickly closing security gaps and at the same time enabling all market participants to be informed in due time about future changes.

Furthermore, the definition of the reference offer, as foreseen under the DMA, is of utmost importance to ensure a clear and operative specification for actors willing to interoperate. In this report, BEREC provides a first list of minimum criteria to be included in the offer, such as service level agreements and guarantees, key performance indicators including threshold values, as well as other relevant technical information. BEREC remains at the disposal of the European Commission (EC) to determine whether the technical details and the general terms and conditions published in the gatekeeper's reference offer ensures compliance with the interoperability obligation in the DMA.

Finally, the report shows how the interoperability provisions under the DMA and the EECC share a similar objective, but work in a different, complementary way. While Article 7 DMA will likely apply first, Article 61(2) EECC may complement this regulatory intervention in cases where end-to-end connectivity are deemed to be endangered, or when the conditions/thresholds for imposing the measure and thus reaching the given objective are only met under the EECC. In any case, BEREC believes that the coherence between the two regulatory frameworks will be ensured through the respective governance structures: the EC has a leading role in both cases and BEREC's involvement will further contribute to fostering consistency.



1. Introduction

Number-Independent Interpersonal Communication Services (NI-ICS) typically include messaging, video-conferencing and e-mail services. Their use has drastically increased in the last decade and NI-ICS have now become a crucial means of communication for a variety of different users throughout Europe.

Article 7 of the Digital Markets Act¹ (DMA) and Article 61(2)(c) of the European Electronic Communications Code² (EECC) include provisions for specific NI-ICS providers to make their services interoperable.

In this report, BEREC explores and analyses the objectives, the scope and the “triggers” of interoperability obligations under the DMA and the EECC, the potential technical approaches and the implementation challenges to be taken into account, as well as the interplay between the two regulatory frameworks. A BEREC report on this interplay was published in 2021³.

While the DMA interoperability obligation can apply to all types of NI-ICS, the legislative discussions mainly concerned messaging services. In order to ensure early and timely input to the European Commission for the enforcement of the DMA, the present report mainly focuses on interoperability for messaging services. The interoperability between other types of NI-ICS, such as videoconferencing services, could be analysed more in depth by BEREC in the future.

On top of its work on the implementation of the EECC, BEREC has already worked on topics related to the digital economy. BEREC also extensively contributed to the European debate and legislative proposals concerning digital gatekeepers⁴. Moreover, in 2021 BEREC

¹ Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925>

² Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code, 17.12.2018.

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L1972>.

³ BoR (21) 85, BEREC Report on the interplay between the EECC and the EC's proposal for a Digital Markets Act concerning number-independent interpersonal communication services, 10.06.2021, see Section 3.

<https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-interplay-between-the-eecc-and-the-ecs-proposal-for-a-digital-markets-act-concerning-number-independent-interpersonal-communication-services>

⁴ BoR (21) 130, BEREC Report on the outcome of the public consultation on the Draft BEREC Report on the ex-ante regulation of digital gatekeepers, 30.09.2021.

https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/10042-berec-report-on-the-outcome-of-the-public-consultation-on-the-draft-berec-report-on-the-ex-ante-regulation-of-digital-gatekeepers;

BoR (21) 131, BEREC Report on the ex ante regulation of digital gatekeepers, 30.09.2021,

<https://berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-ex-ante-regulation-of-digital-gatekeepers>; <https://berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-ex-ante-regulation-of-digital-gatekeepers>;

BoR (21) 93, BEREC proposal on the set-up of an Advisory Board in the context of the Digital Markets Act, 10.06.2021.

commissioned a study on EU consumer perceptions and behaviour on digital platforms for communication⁵ and published a report on the interplay between the EECC and the EC's proposal for a DMA concerning NI-ICS⁶. BEREC has also worked on the definition of guidelines concerning the minimum criteria for a reference offer⁷. While this work on reference offers was more specifically related to the traditional electronic communications market, BEREC's expertise on the topic can contribute to determining whether the technical details and the general terms and conditions published in the gatekeeper's reference offer ensures compliance with the DMA obligation.⁸

This document is organised as follows. Chapter 2 presents the definition of NI-ICS and clarifies the scope of the report. Chapters 3 and 4 focus on the economic and behavioural features, as well as the state of the market of messaging services. Chapter 5 details the different technical approaches to apply interoperability measures and the implementation challenges which should be taken into account. Chapters 6 and 7 present interoperability obligations under the DMA and the ECS regulatory framework, respectively. Chapter 8 provides some insights on the interplay between these two regulatory frameworks. Chapter 9 focuses on potential future work on related topics and Chapter 10 concludes.

Please note that along this report, when referring to “end-users” and “business users”, BEREC is following the same definition as in the DMA and in the BEREC Report on the Internet Ecosystem⁹. Thus, for the purpose of this report, “end-user” means any natural or legal person

https://berec.europa.eu/eng/document_register/subject_matter/berec/others/9963-berec-proposal-on-the-set-up-of-an-advisory-board-in-the-context-of-the-digital-markets-act;

BoR (21) 94, BEREC proposal on remedies-tailoring and structured participation processes for stakeholders in the context of the Digital Markets Act, 10.06 2021.

https://berec.europa.eu/eng/document_register/subject_matter/berec/others/9964-berec-proposal-on-remedies-tailoring-and-structured-participation-processes-for-stakeholders-in-the-context-of-the-digital-markets-act;

BoR (20) 138, BEREC Response to the Public Consultations on the Digital Services Act Package and the New Competition Tool, 08.09 2020.

<https://berec.europa.eu/en/document-categories/berec/others/berec-response-to-the-public-consultations-on-the-digital-services-act-package-and-the-new-competition-tool>;

BoR (18) 35, BEREC Report on the impact of premium content on ECS markets and the effect of devices on the open use of the internet, 08.03.2018.

<https://berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-impact-of-premium-content-on-ecs-markets-and-the-effect-of-devices-on-the-open-use-of-the-internet>

⁵ BoR (21) 89, PPMi Report: Analysing EU consumer perception and behaviour on digital platforms for communications, 11.06.2021.

<https://berec.europa.eu/en/document-categories/berec/reports/analysing-eu-consumer-perceptions-and-behaviour-on-digital-platforms-for-communication-analysis-report>

⁶ BoR (21) 85, BEREC Report on the interplay between the EECC and the EC's proposal for a Digital Market Act concerning number-independent interpersonal communication services, 11.06.2021.

<https://berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-interplay-between-the-eecc-and-the-ecs-proposal-for-a-digital-markets-act-concerning-number-independent-interpersonal-communication-services>

⁷ BoR (19) 238, BEREC Guidelines on the minimum criteria for a reference offer relating to obligations of transparency, 05.12.2019.

<https://www.berec.europa.eu/en/document-categories/berec/regulatory-best-practices/guidelines/berec-guidelines-on-the-minimum-criteria-for-a-reference-offer-relating-to-obligations-of-transparency>

⁸ As foreseen in Recital (64) DMA Ibid footnote 1

⁹ <https://berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-internet-ecosystem>.

using services other than a business user and “business user” means any natural or legal person acting in a commercial or professional capacity using services for the purpose of or in the course of providing goods or services to end-users. When using “users” hereafter, BEREC refers to both end-users and business users. This definition of “end-user” differs from the one in Art. 2(14) of the EECC where “end-user” means a user not providing public electronic communications networks (ECNs) or publicly available electronic communications services (ECSs).

In this report, BEREC uses the term “key providers” to refer to those providers of NI-ICS which meet the criteria identified in Article 61(2)c EECC¹⁰. The criteria used in this article for defining providers subject to the corresponding obligation differ from the criteria used to designate “gatekeepers” according to the quantitative thresholds and qualitative criteria under Article 3 of the DMA, as well as from the definition of undertakings with Significant Market Power (SMP) as defined under Article 63 EECC.

2. NI-ICS and scope of the report

2.1. Definition

Interpersonal communication services (ICS)¹¹ encompass two types of services: number-based (NB-ICS) and number-independent ICS (NI-ICS). Specifically, the EECC defines NI-ICS as an interpersonal communication service which does not connect with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which does not enable communication with a number or numbers in national or international numbering plans.¹²

2.2. Categories

NI-ICS can be considered according to their functionalities or the type of service/s provided.

Concerning the functionalities, NI-ICS typically offer sharing of text messages, images, voice messages, videos and other attached files in end-to-end communication between two individual end-users or within groups of individual end-users, and end-to-end voice and video calls between two individual end-users or between a group and an individual end-user.

¹⁰ See chapter 7

¹¹ I.e. a service “normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service” (Art. 2 of the EECC, Ibid footnote 2)

¹² For further insights on the EECC definitions of the services, Ibid footnote 2

Concerning the service provided, NI-ICS include messaging services¹³, videoconferencing services and email services. Table 1 presents both, the categories of service and the main functionalities/features in each category. While the categories are not always clear-cut (e.g., messaging services often integrate voice and video call functionalities), the categories group together similar services for similar use cases.

The functionalities of the different categories may evolve over time. On the one hand, the scope of functions of email as a standardised service has not expanded to a significant extent so far¹⁴, and for example secure end-to-end encryption across the board is not implemented. On the other hand, messaging services were initially restricted to sending text messages, but they now offer a variety of functions such as the ability to send voice messages and pictures, end-to-end encryption, group chats and other functions. Videoconferencing services are focused on real-time communication among users. Commercial products focused on videoconferencing services are often primarily targeted at professional settings, such as work meetings or online training, and offer enhanced video calling features such as large group video calling, session recordings, screen sharing and virtual backgrounds. In terms of functions offered, messaging and videoconferencing services may also partly overlap, since users can use functions of both service categories for similar purposes (e.g., video calling features).

The majority of services can be used on both, computers (laptop or desktop) and mobile devices (e.g., smartphones or tablets), often by using the corresponding (native or web) applications of the service provider.

Many NI-ICS are provided at no direct monetary cost for users¹⁵. Their business model may rely on users' subscription or users' data monetisation, and subsequent targeted display advertising. When data are collected, they may also be used within the same provider-specific ecosystem to improve other products and services, and targeted advertising. Demand synergies with other (monetised) services or products, for example devices and/or operating systems, can also be a reason to provide NI-ICS. Further insight on the NI-ICS business models and revenues sources can be found in the BEREC Report on NI-ICS revenue indicators.¹⁶

¹³ The category of messaging services in this report covers only NI-ICS and therefore does not include NB-ICS like short message services (SMS) or Multimedia Messaging Service (MMS).

¹⁴ This could also be explained by the fact that e-mail services may have converged to the basic utility which is expected and needed by the users

¹⁵ Nevertheless, some NI-ICS, for example videoconferencing services, charge users for the service, often within a "freemium" business model, which provides only basic functionalities without monetary costs to users.

¹⁶ BoR (22) 183, BEREC Report on number-independent interpersonal communication services (NI-ICS) revenue indicators, <https://berec.europa.eu/en/document-categories/berec/reports/report-on-number-independent-interpersonal-communication-services-ni-ics-revenue-indicators>.

Table 1: Comparison of different types of services in terms of features

	Messaging Services	Videoconferencing Services	E-mail Services
TYPE OF COMMUNICATION	Predominantly asynchronous	Predominantly synchronous	Asynchronous
POSSIBLE FEATURES¹⁷	<ul style="list-style-type: none"> - Text Messages (1:1; 1:n) - Voice and video calling (1:1; 1:n), Sending Pictures, voice messages, GIF, Videos, Documents - Sharing of Location - Self-destructing messages - Complementary (often non-communication) functions such as conversational commerce, payment, In-App-Gaming etc. 	<ul style="list-style-type: none"> - Voice and video calling (1:1; 1:n) - Text Messages - Screen Sharing - Whiteboarding - Application Sharing - Application integration (e.g., calendar) - Temporary handover of application control - Accessibility (display of user's availability and location information) - Different meeting rooms <ul style="list-style-type: none"> - Session recording - Virtual Backgrounds - Dialling-in by phone numbers 	<ul style="list-style-type: none"> - Text messages (1:1; 1:n) - Sending Pictures and Documents - Read Receipts and related analytics information - When using Webmail: Integration of complementary services (e.g., calendar)
TECHNICAL STRUCTURE (ARCHITECTURE)	Predominantly centralised server architecture	Predominantly centralised server architecture	Federated server architecture (different providers)
ENCRYPTION	Transport Encryption: TLS-Protocol; End-to-End-Encryption (1:1): e.g. Double-Ratchet Protocol; End-to-End Encryption (1:n): Often only possible to a limited extent	Transport Encryption: TLS-Protocol ; End-to-End-Encryption: The possibility of dialling in by phone makes end-to-end encryption significantly more difficult.	Transport Encryption: TLS-Protocol; End-to-End-Encryption: No direct end-to-end encryption integrated in common email standards (Possibility of End-to-End-Encryption by using additional standards/programs (e.g., S/MIME or PGP))
INTEROPERABILITY	Currently no interoperability between most frequently used applications within this category	Currently no interoperability between most frequently used applications within this	Interoperability between different e-mail providers due to internet standard communication protocols (SMTP/IMAP)

¹⁷ The list is not exhaustive

		category, although some cases are implemented ¹⁸	
--	--	---	--

2.3. Scope of the report

As described in the previous section, NI-ICS provide a variety of different functionalities, such as text messages, sharing of images, voice messages and videos, as well as voice and video calls.

The DMA identifies a schedule for the implementation of interoperability obligations with respect to basic functionalities provided by the gatekeeper¹⁹: after providing a reference offer, end-to-end text messaging and sharing of any attached file (images, videos, voice messages or any other) shall be made interoperable within six months after the gatekeeper designation for communication between two individual end-users, and within two years for communication among users within groups. Voice and video calls are to be implemented within four years after the gatekeeper designation.

While the DMA interoperability obligation can apply to all types of NI-ICS, the legislative discussions mainly concerned messaging services. In order to ensure early and timely input to the EC for the enforcement of the DMA, the present report mainly focuses on messaging services. The interoperability between other types of NI-ICS, such as videoconferencing services, could be analysed more in depth by BEREC in the future.

With regard to e-mail services, technical interoperability is already in place and based on standardised formats and protocols (SMTP, IMAP). This does not mean that there may not be potential issues concerning effective interoperability and in a broader but related scope migration and switching²⁰. For instance, some constraints may be imposed by the providers for security or spam-protection reasons, *de facto* limiting server-to-server communications. This report does not cover these aspects, but they may be explored in the future by BEREC.

3. Economic and behavioural features of messaging services

The use of online messaging services has become widespread and they have been increasingly used together with and often instead of traditional communication services (especially SMS). Overall, the availability and use of messaging services has contributed to a

¹⁸ Shaw, N., Streamline your communications experience with direct guest join from Zoom and Microsoft, 2022, https://blog.zoom.us/direct-guest-join/?utm_source=social&utm_medium=organic-social&utm_campaign

¹⁹ Article 7 DMA Ibid footnote 1

²⁰ The EECC explicitly addressed email switching. See, for instance, annex VI Part B (b).

significant change in the behaviour of telecommunications users, both in terms of the type of communication and its intensity.

The adoption of messaging services next to telephony and SMS seems to be more strongly driven by the added features and functions these services offer to users than solely to messaging services being a cheaper (e.g., for international calls or messages) or a better means to fulfil the same communication need. Several studies²¹ have linked different usage patterns of specific services to meet different needs, by choosing certain services to connect with particular groups of people to keep their communication circles separate and e.g. keep their professional and their family contacts on the different services. Surveys²² also show that most end-users tend to communicate via multiple applications at the same time and that the preferred communication means often replace one another in different situations, arguing that the contacts that end-users have on a specific application affect their conversations, their communication patterns with the application, and the quality of their social relationships.

For messaging services, multi-homing²³ appears to be widely spread. In theory, this can favour competition among different providers since users could benefit from differentiated products or service features. However, it should be noted that multi-homing does not necessarily mean that the related market is competitive. For instance, the most used messaging applications belong to the same undertaking (e.g. WhatsApp and Facebook Messenger belong to Meta, and Facetime and iMessage to Apple).

Network effects and free-of-monetary-charge use seem to be the main and rather decisive criteria for users when choosing a messaging application.²⁴ Network effects are self-reinforcing and confer a competitive advantage to those services which reach a critical mass of users. Taking also into account the high user-friendliness of these messaging services, they have become particularly attractive to a large number of users. Group features reinforce even more these network effects, as switching from an application to another could entail significant coordination costs. For instance, when one member of a group chat wants to switch to a different service, all participants in a group chat on a specific messaging service should switch, if users want to keep communicating to all the members of the group. On top of procedural switching costs (time to adapt) and convenience of use, relational switching costs (fear to lose usual communication partners) appear to be an additional barrier to changing service. Network effects can therefore cause lock-in effects likely resulting in lower competition between providers of messaging services as well as limited contestability. Entry barriers could also be present due to the existing established critical mass.

²¹ See for instance Arnold, R, Schneider, A, Lennartz J, Interoperability of interpersonal communications services A consumer perspective, 2020. <https://www.sciencedirect.com/science/article/abs/pii/S0308596120300197>

²² Ibid footnote 5

²³ A situation in which users use more than one application for similar purposes, and switch between them according to their needs

²⁴ Ibid footnote 5



Moreover, low switching could also be explained by user inertia.²⁵ In this respect, despite the trend towards multi-homing on applications for messaging services and social networking sites, consumers' behaviour in relation to their main applications remains stable. PPMI's analysis report for BEREC on "Consumer perceptions and behaviour on digital platforms"²⁶ shows that end-users appear to develop a strong attachment and loyalty towards their preferred communication application, viewed from various perspectives. This provides strong evidence of consumer inertia, brand identification and emotional attachment to applications, which constitute the key single-homing²⁷ factors with regard to messaging services.

When choosing their main messaging application, other criteria such as the additional offered features in the service, the convenience of use, privacy or the security of data²⁸ and the extent of data collection practices are considered by users, but to a significantly lesser extent than network effects and free-of-charge use.

As regards data privacy and security in particular, even though respondents in surveys across various demographics state that they consider them to be important, strong data privacy and security standards on messaging services seem in the end to be less important to end-users than the ease and convenience of messaging services, contacts already using them, and being able to use them free of charge. This behaviour is reported as the "privacy paradox": the discrepancy between users' intentions to protect their privacy and the way they actually behave online. However, their actual behaviour may also be due to/influenced by the practices of the service providers (e.g., it may be difficult not to accept some terms and conditions if this would result in being excluded from the platform). As regards the intensity of data collection, while some users have concerns about the use of their data for marketing purposes, most of them "accept the reality" that providers use their data in exchange for communication services, and were not overly concerned in practice about privacy issues involved, or are not adequately assessing them. This factor may involve users rationalising the use of digital platforms, though without taking additional data precautions or adopting more protective behaviours. All these factors contribute to strengthening consumer inertia, which coupled with network effects results in market concentration.

Another factor to consider is that the major messaging services providers are often part of provider-specific ecosystems in which several services are provided by the same company and closely integrated (e.g., Meta provides both WhatsApp and Facebook Messenger, Apple

²⁵ A report published by RTR on switching barriers for key internet services, provides the following data on switching behaviour between different services, based on a survey: In the last two years, only 6% of the respondents have changed the messenger they mainly use. In contrast, 19% of the respondents have switched their mobile phone tariff provider, 8% the browser and 5% the search engine they mainly use on their mobile phone. RTR, Switching barriers for key Internet services, 2022.

https://www.rtr.at/TKP/aktuelles/publikationen/publikationen/switching_barriers.en.html

²⁶ Ibid footnote 5

²⁷ Ibid footnote 5. The tendency of users to adopt and continue using a single application or service is known as mooring or single-homing. Several studies employ the theory of Push-Pull-Mooring (PPM) to distinguish between the movements of users in different directions and the tendencies to moor or home within a specific platform.

²⁸ Ibid footnote 21

provides Facetime and iMessage, which are bundled with and only work on Apple devices). This can further reinforce lock-in effects, switching costs and consumer inertia, and represent an additional barrier to entry and contestability²⁹.

4. The state of the market for messaging services

This chapter gives a general overview of the market for NI-ICS and especially for messaging services. It mainly focuses on some key figures, namely on the main messaging services used, how often people use messaging services and to what extent people multi-home. A more detailed description of the residential market for messaging services can be found in the PPMI report.³⁰ Concerning the business segments, BEREC has explored the use of collaborative tools, including messaging services, in the study on Communication Services for Businesses in Europe.³¹

4.1. Main applications/actors

The most widely used applications among European end-users in 2020 were WhatsApp, selected as the main application by over 61% of end-users, followed by Facebook Messenger, selected by nearly 23% of end-users.³² WhatsApp is the most popular messaging service within all the age groups surveyed³³ and it differs per Member State whether respectively WhatsApp or Facebook Messenger is the messaging service used the most.³⁴ As both these services belong to Meta, there seems to be a high concentration in the market for messaging services.³⁵

Figure 1: The main applications identified by European end-users for interpersonal communications³⁶, 2020 data

²⁹ BoR (22) 167, BEREC Report on the Internet Ecosystem, <https://berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-internet-ecosystem>

³⁰ Ibid footnote 5

³¹ BoR (22) 184, Study on Communication Services for Businesses in Europe: Status Quo and Future Trends, <https://berec.europa.eu/en/document-categories/berec/others/external-study-on-communication-services-for-businesses-in-europe-status-quo-and-future-trends>

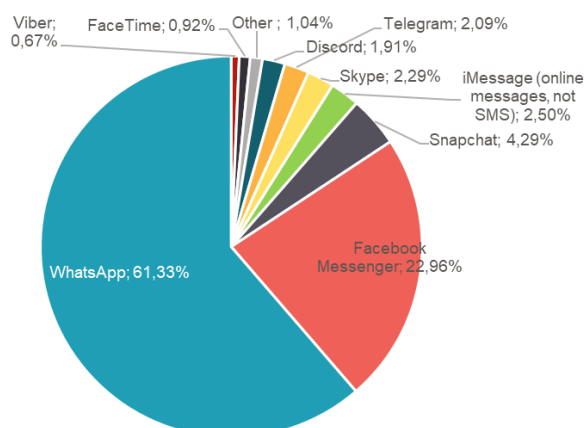
³² Ibid footnote 5, figure 16.

³³ Ibid footnote 5, figure 17.

³⁴ Ibid footnote 5, figure 20.

³⁵ Instagram Direct Messaging was not mentioned in this report

³⁶ Ibid footnote 5, figure 16.



Source: PPMI's analysis report Analysis of Q11: "Over the past 3 months, which of these online websites or applications did you use most frequently?"

4.2. Use of messaging services

72% of the European end-users using WhatsApp do so on a daily basis. For Facebook Messenger this holds for 50%.³⁷ This use of messaging services has increased over the past period. 45% of end-users state that their use of messaging services increased over the preceding 12 months. Only 6% indicate a decrease.³⁸ The usage has also increased rapidly since the Covid-19 lockdown.³⁹

With the development of messaging services, communication behaviours have changed. The increased use of these messaging services triggered a decrease in the use of SMS, mobile and fixed phone calls. 60% of end-users state they make fewer calls or send fewer SMS because of the use of messaging services.⁴⁰ The same conclusion follows when looking at the decline of the numbers of SMS sent: the SMS volume decreased with almost 65% since 2012.⁴¹

People use different means of communication in different situations. For cross-border communication, 71% of the respondents indicate they use messaging services exclusively, while only 14% indicate to use traditional means of communication exclusively. For their day-

³⁷ Ibid footnote 5

³⁸ Ibid footnote 5, figure 43.

³⁹ ITU, Economic impact of covid-19 and the digital infrastructure, 2020, p. 9. https://www.itu.int/pub/D-PREF-EF.COV_ECO_IMPACT-2020 and Seuffer, A., Poignee, F. & Seufert, M., Pandemic in the digital age: analysing WhatsApp communications behaviour before, during, and after the COVID-19 lockdown, Humanities and Social Sciences Communications, 2022, <https://www.nature.com/articles/s41599-022-01161-0>

⁴⁰ Ibid footnote 5, figure 53.

⁴¹ BoR (21) 159, BEREC Report on termination rates at European level- 30 June 2021, 09.12.2021. <https://www.berec.europa.eu/en/document-categories/berec/reports/report-on-termination-rates-at-the-european-level-30-june-2021>

to-day communication with friends and family, 53% indicate they use messaging services exclusively.⁴² This is also confirmed in a study by the EC in 2018, which states that people use the internet applications more for international communication than they use mobile or fixed telephony services.⁴³

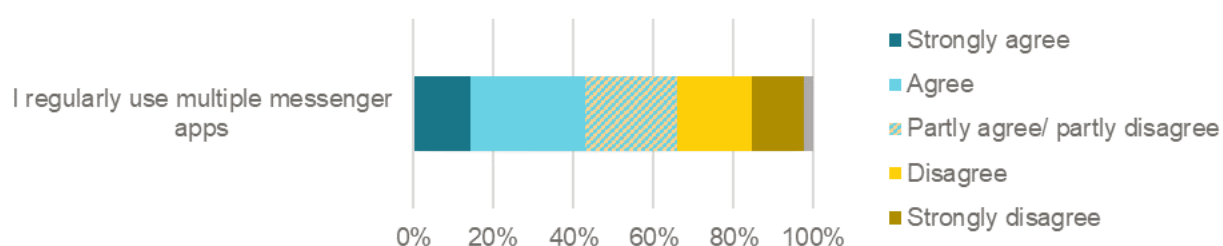
Also, when in touch with one or more persons and for different age groups, traditional means of communication are seldom used: only 11% indicate using traditional means exclusively, against 54% who indicate that they prefer messaging services exclusively. In contrast, end-users prefer traditional communication in case they need urgent, private or secure communication.⁴⁴

People use messaging services for various functionalities. Text messages and voice calls are the most widely used functionalities among users of WhatsApp, Facebook Messenger and Skype. This holds for all demographic groups. Meanwhile, application functionalities such as group messages and calls, video calls and the exchange of files, are much more popular among younger users, especially among those primarily using WhatsApp and Facebook Messenger.⁴⁵

4.3. Multi-homing

A large part of European citizens multi-home in the use of messaging services. However, the frequency of use of specific applications must be considered when trying to assess multi-homing between different applications. For instance, more than 82% of the end-users use two or more messaging services at least once a month, but only 48% of them use at least two of these applications daily.^{46, 47}

Figure 2: Regular use of multiple messenger applications



⁴² Ibid footnote 5, figure 55.

⁴³ EC, July 2018, Eurobarometer: E-communications and digital single market- Publication Reports, page 98-99 [E-communications and digital single market juli 2018 - Eurobarometer survey \(europa.eu\)](https://ec.europa.eu/eurobarometer/surveys/index.cfm?id=689)

⁴⁴ Ibid footnote 5, figure 55.

⁴⁵ Ibid footnote 5, figure 13.

⁴⁶ Ibid footnote 5, figure 15.

⁴⁷ Ibid footnote 5, Data from PPMI database, calculations by BEREC.

Source: PPMI's analysis report Analysis of Q24: "I regularly use multiple messenger applications".

For respondents who stated a daily use of only two different applications, in over 94 % of the cases these applications were either WhatsApp or Facebook Messenger. According to the study prepared by PPMi for BEREC, as the number of multi-homed applications grows, the likelihood of one of the applications used being either WhatsApp or Facebook Messenger keeps rising. For all daily multi-homers (using up to 5 applications daily), just 5% said they did not use WhatsApp nor Facebook Messenger, while almost half of them used both applications.⁴⁸

5. Interoperability measures

5.1. Objectives and types of interoperability measures

Interoperability is "*the ability of two or more systems or components to exchange information and to use the information that has been exchanged*"⁴⁹. Interoperability does not require interoperable systems or components to be uniform, but requires some common understanding on the exchange of information, e.g. via interfaces or standards. In order to be interoperable, undertakings providing systems or components set interfaces or implement standards at the edge of their services and products in order to allow the exchange and use of information.

Interoperability is not an end in itself, but a means to reach specific objectives⁵⁰. The definition set above encompasses a large array of practices. Kerber and Schweitzer⁵¹ identify three reasons for the imposition of interoperability: (i) market failure due to a dominant provider, which has the ability and may have the incentive to foreclose access of downstream providers to non-duplicable infrastructure; (ii) market failure due to network effects, which may lead to tipping of the market to the largest network; and (iii) to enable connectivity between all members of society in line with universal service considerations.

It is important to distinguish between horizontal interoperability and vertical interoperability⁵².

⁴⁸ Ibid footnote 5, Data from PPMI database, calculations by BEREC.

⁴⁹ IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries, 1990, page 42. http://www.mit.jyu.fi/ope/kurssit/TIES462/Materiaalit/IEEE_SoftwareEngGlossary.pdf

⁵⁰ The capacity of interoperability measures to reach objectives without presenting important drawbacks (e.g. in terms of competition, innovation, innovation or privacy) depends on the way the measures are implemented.

⁵¹ Kerber. W, Schweitzer. H., Interoperability in the Digital Economy, JIPITEC, 39 para 1, 2017. https://www.jipitec.eu/issues/jipitec-8-1-2017/4531/JIPITEC_8_1_2017_Kerber_Schweitzer.pdf

⁵² For a distinction between vertical and horizontal interoperability, ibid footnote 51 and footnote 4 (BoR (21) 131).

- **Horizontal interoperability**⁵³ means the exchange and use of information between equivalent/substitutable systems or components, possibly provided by competing undertakings. It allows for end-to-end communications or other functions between users of different services, as it is the case for NI-ICS (e.g., messaging services) as foreseen in Article 61(2)(c) of the EECC and Article 7 of the DMA.
- By contrast, **vertical interoperability**⁵⁴ gives complementors or business users access to essential functionalities allowing the development of their services (usually via APIs) to complement those provided by the system which interoperability applies to. Since it does not concern end-to-end connectivity, vertical interoperability is not understood to be within the scope of Article 61(2)(c) of the EECC.⁵⁵ However, the concept may also be relevant for those services which carry complementary and ancillary services, such as services offered to business users or providers of services regarding payments, emojis or GIFs.

As expressed previously, this **report will focus** primarily **on horizontal interoperability**, which concerns end-to-end connectivity or potential lack of competition and is particularly relevant when it comes to NI-ICS. In terms of services, this report looks at interoperability only in the context of **messaging services**.

Horizontal interoperability obligations for messaging services are intended to mitigate the impact of network effects and may help to reduce market concentration.⁵⁶ Without interoperability, network effects are firm-specific and proprietary, which results in firms competing to offer the larger network benefits to users.⁵⁷ Depending on the strength and relevance of network effects for users, the market may eventually tip in favour of one firm.

By contrast, with horizontal interoperability, network effects are shared among providers and are aggregated into market-wide network effects.⁵⁸ Rather than competition for the greatest number of users ("winner-takes-all" effect), firms could compete on other aspects of quality, such as user friendliness, innovative functions or data protection and data security. Interoperability could therefore increase consumer choice in services overall through a reduction of lock-in effects.

⁵³ Also referred to as "*full protocol interoperability*" in the report by Crémer, J, de Montjoye, Y.A, & Schweitzer, H, Competition policy for the digital era, European Commission, 2019.

<https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf>

⁵⁴ Also referred to as "*protocol interoperability*", Ibid footnote 53

⁵⁵ The DMA also foresees vertical interoperability obligations for gatekeepers (Article 6 (7)). Ibid footnote 4 and 1

⁵⁶ Ibid footnote 53, p.59.

⁵⁷ Bourreau, M., Krämer, J., & Buiten, M., Interoperability in Digital Markets. CERRE Report, 2022.

https://cerre.eu/wp-content/uploads/2022/03/220321_CERRE_Report_Interoperability-in-Digital-Markets_FINAL.pdf

⁵⁸ Scott Morton, F. M., Crawford, G. S., Crémer, J., Dinielli, D., Fletcher, A., Heidhues, P., & Seim, K., Equitable Interoperability: the "Super Tool" of Digital Platform Governance, Policy Discussion Paper No. 4, Digital Regulation Project, Yale Tobin Center for Economic Policy, 2021.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3923602

Generally, interoperability can help to avoid foreclosure tendencies in markets by facilitating market access for potential competitors. A new entrant does not need to reach a critical mass of users to offer its service. From the beginning, it can offer access to all users of an existing service through interoperability. Interoperability, therefore, can promote competition between service providers such as that which began, for example, in the course of the liberalisation of the electronic communications markets, when interoperability obligations (manifested in the form of mandated access and interconnection) broke up former state electronic communications monopolies. This enabled competitors to offer their own voice telephony services that also permitted communication with customers of the former monopolists.⁵⁹ This interoperability, together with the fact that NB-ICS are usually provided against payment, often results in single-homing.

5.2. Interoperability approaches

Interoperability for messaging services may come in different degrees, and can be implemented by different technical approaches.⁶⁰ With regard to services being covered by interoperability obligations, it is important to distinguish between a **symmetrical** and an **asymmetrical approach to interoperability**.

- If a **symmetrical approach** is chosen, all service providers would be required to be interoperable, regardless of their size, number of users and their market position. This is the type of approach taken for traditional communication services like telephony and SMS.
- Under an **asymmetric approach**, only some providers of messaging services may be subject to interoperability measures, if they fulfil certain criteria⁶¹. They would be the only ones required to open interfaces to their services. Alternative providers would have the choice of using these interfaces.

Furthermore, with regard to functions, interoperability could come in **different degrees**. Rather than making all functions of messaging services interoperable, obligations could initially focus only on core functions like sending text messages or pictures. More advanced or less used functions would therefore not be covered by interoperability requirements. The degree of interoperability can therefore be defined as the relative extent of interoperable functionalities in messaging services.⁶²

⁵⁹ Interoperability between messaging services an overview of potential and challenges, Federal Network Agency, Germany, 2021.

https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digitales/OnlineKom/diskussionspapier_IOP_EN.pdf?__blob=publicationFile&v=4

⁶⁰ Ibid footnote 57

⁶¹ For example, the designation of gatekeepers under the DMA.

⁶² Ibid footnote 57

There are various **interoperability approaches** that could permit communication between different messaging services. These have technical differences and varying degrees of effort required with respect to the necessary technical conditions. Furthermore, developing solutions for interoperability can be based on different procedures. Private actors may develop and give access to their own technical solutions such as APIs or bridges (see section 5.2.1). Alternatively, solutions can be developed through formal standardisation. Under section 5.2.2, we discuss the pros and cons of standardisation.

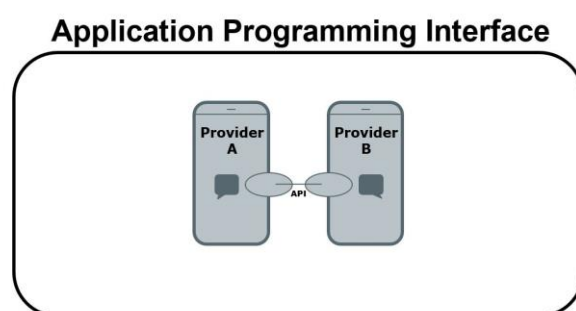
Since interoperability obligations under both Article 61(2)(c) EECC and Article 7 DMA are asymmetric in nature, the following analysis is focused on interoperability requirements only for certain key providers of messaging services meeting the criteria in Article 61(2)(c) EECC or gatekeepers under the DMA.⁶³

5.2.1. Technical solutions

5.2.1.1. Application Programming Interfaces (APIs)

One way of ensuring communication across providers of messaging services is the provision and use of interfaces, also known as APIs. APIs are used to specify which functions are available, which format data are transmitted in, and who can communicate using the interfaces. If a provider makes an interface available for a service via a set of APIs, providers of other services can use it to exchange data, communicate with each other and develop own software using APIs, although this depends on the scope and design of the interface. APIs can be technically different for different providers, as there is no technical reason for different key providers or gatekeepers to use a common set of APIs.

Figure 3: Application Programming Interfaces



Source: BEREC

However, by providing APIs, the key provider or gatekeeper also sets the conditions for interoperability, for example by which means the users are identified (e.g., by telephone

⁶³ See chapters 6 and 7 for legal analysis.

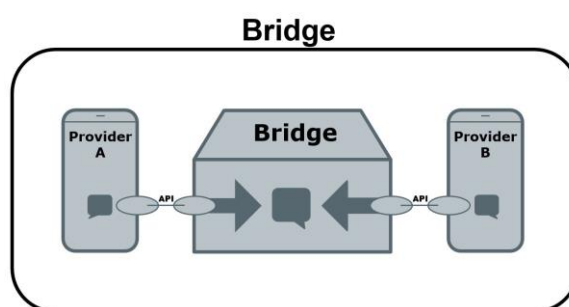
numbers, mail addresses or by other identifiers). There is a risk that smaller and more privacy-focused providers would be limited in their use of the APIs and may have to accept e.g. that the telephone number must be used for identification instead of pseudonymised identifiers. Smaller providers may also be limited in their use of APIs if multiple gatekeepers each have different technical requirements for using the API, making the implementation effort greater than the benefit of interoperability.

Interoperability based on APIs developed by the NI-ICS provider⁶⁴ could preserve the ability to innovate and develop new features as new functions offered by a provider do not automatically have to be designed to be interoperable with existing APIs but APIs can be gradually updated to extend to new functions. Therefore, a process for changing or updating the relevant protocols (e.g., defining transition times, notifying processes before obsolete elements are removed) is necessary. This kind of processes are needed in order to allow third parties stable interactions.

5.2.1.2. Bridges

Another way to enable exchange between different messaging services is the use of bridges. With bridges, different services are not made directly interoperable in a technical sense⁶⁵, but the message stream of two different services are synchronised with each other via the bridge. For this, the bridge acts as a separate translation service between the different messaging services which implements all protocols of both the messaging services and synchronises the message feeds. In the end, communication between different users who use different messaging services would be possible across these services.

Figure 4: Bridge



Source: BEREC

In order to provide a bridge, the actor providing the bridge is dependent on being able to use appropriate interfaces to exchange data between the different messaging services. The use of well-documented APIs could therefore make it easier to implement bridges, since the provider of a bridge then can rely on the already given access conditions. Therefore, bridges

⁶⁴ For standardisation, see section 5.2.2

⁶⁵ Cf. definition of interoperability in chapter 5.1

do not constitute a separate alternative to APIs, as an API is always required to provide a bridge. One advantage of using bridges is that providers of different messaging services do not have to be directly interconnected (e.g., by using APIs). Instead, communication between different messaging services is enabled via the bridge. A bridge as a separate service is also not limited in terms of supported messaging services and therefore could also offer communication among several different messaging services.⁶⁶ Furthermore, since different services are not interoperable directly and bridges can be run as separate services, this also allows to only support certain functions. The integration of new messaging services is also simplified, since only the bridge needs to be adapted. Innovations are also still possible for adjacent functions since bridges only include certain functions. However, if these implemented functions are changed by the providers of messaging services, the bridge needs to be updated, too.

On the downside, when using bridges, the message stream gets transcoded to support different APIs and coding techniques offered by different messaging services. This introduces challenges for end-to-end encryption, data protection and privacy: by the definition of end-to-end encryption, no third party but the senders and receivers of a message should be able to decrypt the data and read or modify it. With the transcoding of messages introduced by bridges, this concept gets abandoned. This may result in a weakened security level, as the provider of a bridge can potentially access communication content. Furthermore, the use of bridges may also pose a challenge in terms of user transparency with regard to data protection and security, because it may not be obvious to end users that they are communicating via a bridge.

Individual market participants have already pursued the development and use of bridges without the need of regulatory intervention. However, the use of this kind of indirect method of creating interoperability can breach the terms of use of the individual messaging services and providers often use technical means to prevent it. In any case, the approach of bridges is already in use within the Matrix messaging protocol⁶⁷ and discussed within the Matrix community⁶⁸.

5.2.2. Standardisation

Technical solutions for ensuring interoperability between different messaging services can be developed through (full) **standardisation**⁶⁹. This involves standardising the transmission, the individual functions and necessary interfaces, and the data formats for the exchange of

⁶⁶ For example, see supported services by Matrix bridges: <https://matrix.org/bridges/>

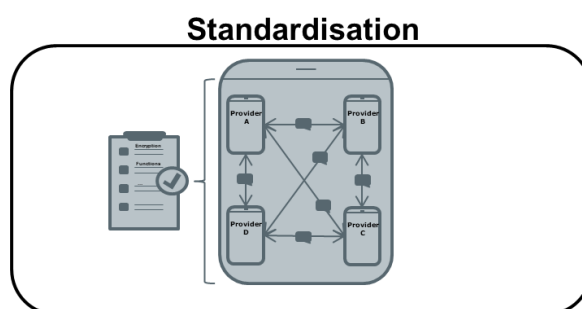
⁶⁷ <https://element.io/enterprise/matrix-bridging-services> [last checked on May 11th, 2022]

⁶⁸ <https://matrix.org/blog/2022/03/29/how-do-you-implement-interoperability-in-a-dma-world> [last checked on May 11th, 2022]

⁶⁹ Strictly speaking, full standardisation is not interoperability in the technical sense, because there is one standardised service that is implemented by all providers. The narrow meaning of interoperability refers to *different* services working together.

information. Standardisation may include APIs which could be used by bridges, as presented above.

Figure 5: Standardisation



Source: BEREC

Full standardisation leads to the development of a standardised service that can then be made available by different service providers and permit users of the different providers to communicate with each other. This is the type of approach that was taken for traditional communication services like telephony and SMS. These standardised services were developed by international standardising bodies and then implemented by the providers. Email services also have standardised formats and protocols (e.g., SMTP, IMAP) so they can be offered by different providers and used to communicate regardless of provider. There are also initiatives to develop open standards in the messaging sector, such as Matrix⁷⁰ and XMPP⁷¹. Open communication protocols are intended to enable use across providers, in a similar way as for email services.

However, this approach requires a high development effort and may be limited in terms of dynamic changes (e.g. new features, closing security gaps in the short term), as different providers would always have to agree on the lowest common denominator (standard) and extensions to this lowest common denominator either need to also be standardised or risk of being implemented platform-specific, leading users to stay with a certain service in order to use all of its functionality. This may reinforce already existing lock-in effects. This being said, technically it is already possible to foresee extensions in the standard, so that new functionalities can be easily introduced while allowing “graceful degradation” for clients not supporting these functionalities.

5.3. Implementation challenges

Several challenges need to be considered for the practical implementation of interoperability obligations. In particular, the technical requirements are decisive for a targeted interoperability

⁷⁰ See Matrix (2022): This is Matrix, available at <https://matrix.org/https://matrix.org/>

⁷¹ See XMPP (2022): Extensible Messaging and Presence Protocol, available at <https://xmpp.org/https://xmpp.org/>

implementation. The following section outlines general implementation challenges of interoperability obligations and briefly describes how they can be potentially overcome. Where necessary, a distinction is made in the explanations with regard to the different technical interoperability approaches already described.

5.3.1. Specifying the interoperability approach and interoperable functions

As a first step, depending on the objectives, a general interoperability approach has to be selected. This means that there needs to be a decision on the addressees of any interoperability obligations and the functions that have to be interoperable. In addition, relevant interfaces and standards to be used (e.g., communications protocols) need to be defined. A common understanding of the technical implementation of interoperability can help to reduce the implementation effort for all providers involved, both for the provider with the obligation to interoperate and third-party providers willing voluntarily to interconnect (see Section 5.2).

The technical design also determines which functions are made available in an interoperable way. It should be taken into account that the range of functions provided is large enough to make the interoperable services attractive to users. Functions that are not made interoperable could reduce the attractiveness of these services, since users are more likely to opt for the service that includes the full range of functions.⁷²

5.3.2. Ensuring innovation in an interoperable environment

At the same time, the specifications for interoperability must be flexible enough to allow for future innovations. In an interoperable system with multiple service providers, it is often only possible to implement dynamic adjustments and innovations (such as expanding the range of functions, changing encryption and communications protocols, or coding methods to improve the service quality) to a limited extent or with a delay, because all market participants have to be informed of such changes in advance.

Therefore, there is concern that overly rigid requirements for implementing interoperability could inhibit future innovation. The interoperable electronic communication service SMS offers an example: NB-ICS users can exchange text messages independently of the provider, but, unlike messaging services, SMS functionalities have hardly evolved in the past.

Messaging services have developed in a dynamic manner, also because they were not submitted to lengthy standardisation procedures. Against this, it is argued that, for example, in the case of the interoperable and standardised e-mail service, there are subsequent adaptations. For example, end-to-end encryption is possible with e-mail services, which was

⁷² Ibid footnote 57



not envisaged at the beginning of the standardisation process. However, today it can be observed that this subsequent extension is hardly used.⁷³

These two examples show that by agreeing on a standard, certain technical specifications and the scope of functions can be defined, albeit at the current state of the art in each case. Innovations can be hampered by this when standards are not formulated with sufficient flexibility. To reduce these potential negative aspects of interoperability on innovations, a differentiated interoperability approach could be considered, focusing only on core functions. Rather than making all functions of messaging services interoperable, any obligations could initially focus on long-established core functions, such as text-based messaging between end users.

With regard to the technical interoperability approach chosen, full standardisation leads to the development of a standardised service in which interoperable functions are set by the standard. This means that changes are only possible via a standardisation process, which might restrict differentiation and innovation possibilities. In contrast, when relying on an API or bridge approach to interoperability, innovations are still possible beyond interoperable core functions, but would not be interoperable by default. In any case, the chosen interoperability approach should provide for an updating mechanism which takes into account adding new functions, closing security gaps quickly and at the same time enables all market participants to be informed about future changes.

5.3.3. Ensuring a high level of data protection and security

Horizontal interoperability between different messaging services also requires that certain user data is exchanged. It is often discussed, if interoperability of messaging services would lead to higher or lower data protection of users. With the introduction of interoperability, the data collection would not increase per se, but it leads to the sharing of (communications and meta-) data⁷⁴ among the different service providers or providers of bridge services in any case.⁷⁵

Without a privacy-by-design approach, the data collection would not decrease compared to current services. If a fully standardised approach was chosen, there is at least the possibility to introduce such privacy-by-design approach. The data necessary to collect for providing a

⁷³ See for example Stransky, C., Wiese, O., Roth, V., Acar Y., Fahl, S. (2022): 27 Years and 81 Million Opportunities Later: Investigating the Use of Email Encryption for an Entire University. 43rd IEEE Symposium on Security and Privacy, IEEE S&P 2022, May 22-26, 2022, available under <https://teamusec.de/pdf/conf-oakland-stransky22.pdf>

⁷⁴ For an in-depth discussion of metadata, see the Federal Office for Information Security (BSI) (2021): Moderne Messenger heute verschlüsselt, morgen interoperabel? P. 12. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/messenger.pdf?__blob=publicationFile&v=8

⁷⁵ Cyphers, B. & Doctorow, C., Privacy without monopoly: Data Protection and Interoperability, 2021. <https://www.eff.org/wp/interoperability-and-privacy#Risksandmitigations> and Doctorow, C. The GDPR, Privacy and Monopoly, 2021. <https://www.eff.org/deeplinks/2021/06/gdpr-privacy-and-monopoly>

service could be reduced to a very minimum, however it may be questionable if anonymity, or at least pseudonymity, could be established.

Registration with messaging services is largely done by disclosing voluntary data for unique identification. Telephone numbers in particular are often used by services as a common identifier, as these are often already available in the local address book of the mobile phone and thus a comparatively simple "contact discovery" can be carried out. With regard to the data sharing and authentication among different interoperable services, the consent of the users to approve the exchange and processing of data to a third-party service needs to be clarified, e.g. if opt-out is possible or opt-in is obligatory.

Nevertheless, interoperability might allow users to switch to services which have better policies regarding confidentiality. But it could also be expected from interoperability that users would resort to only one service (or a few) instead of several services (since multi-homing might not be necessary anymore, or it is resorted to for purposes other than being able to communicate with others in different applications). Hence, users would need to sign up to fewer services, agree to less terms and conditions (notably related to personal data collection), and install fewer applications on their devices. This potentially could result in a lower number of applications collecting data (while active or in the background).

This reduction of differentiating factors could be similar for security standards. At the moment, different levels of encryption exist for different messaging services. Some messaging services support encrypted group chats or video calls, with different group sizes and feature sets. At the moment, there is no common standard for the exchange of cryptographic keys or encryption commonly supported by all providers of messaging services.

It should be noted that the most used services implement the same end-to-end encryption standard (for example, the "Signal Protocol" (formerly known as "axolotl protocol")⁷⁶ is used by Signal, WhatsApp⁷⁷ or optionally Skype⁷⁸), even though they may not necessarily implement it in the same way. For example, many different messaging services set different limitations on group functions. This may be a result of different encryption methods for groups. Large groups are especially challenging for encryption protocols and devices since often they are implemented in a way that every user encrypts messages for every other single user in the group. This leads to high demand of resources which does not scale very well for large groups. As a consequence, encryption could in theory be interoperable and allow different services to communicate securely to some extent.

However, to achieve this, a common standard must be set first (also in the case of an API-approach to interoperability) and used by different providers of messaging services for key-

⁷⁶ Signal, Signal on the outside, Signal on the inside, 2016.

<https://signal.org/blog/signal-inside-and-out/> <https://signal.org/blog/signal-inside-and-out/>

⁷⁷ <https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf>

⁷⁸ Signal, Signal partners with Microsoft to bring end-to-end encryption to Skype, 2018.

<https://signal.org/blog/skype-partnership/> <https://signal.org/blog/skype-partnership/>

exchange and encryption. As already explained, the use of bridges run by third parties to make communication of end users among different messaging services possible, is generally not compatible with end-to-end encryption.

A general challenge with encryption in interoperable (especially in decentralised/federated) environments is that it often results in a minimalist consensus. This could lead to protocols that, for the sake of backwards-compatibility, allow the use of encryption standards that may not be state of the art. Adaptations because of vulnerabilities may be very complex to implement, and innovations may be held back or be implemented very slowly because of the standardisation efforts and compatibility issues (c.f. e-mail, 2G/3G cellular networks).

Protocols like MLS (Messaging Layer Security) may help to solve such issues, but the status and maturity of this protocol is unclear at the moment.⁷⁹ As of September 2022, the publication of the architecture document was requested at IETF as informational⁸⁰ and the publication of the protocol was requested as a *proposed* standard⁸¹, but not finally published yet.

Additionally, it needs to be discussed how exchange of cryptographic keys can be done in an interoperable environment. When many different actors want to participate in such a federated system, the trust of all the parties and the different implementations need to be taken into account. For example, the management of the encryption keys is currently done by a trusted party, the messaging service provider itself. In an interoperable situation, when different service providers participate in this key exchange and management, a centralised institution may be necessary. This could theoretically be carried out by the gatekeeper or by a third party, but this could come with pitfalls such as necessary trust and data protection issues. However, in general, interoperability does not interfere with or prohibit encryption. Standardisation does not automatically lead to slow implementation of state of the art and modern standards and thus “less secure” applications. But implementing end-to-end encryption in interoperable environments comes with many challenges which may lead to an increased complexity.

Finally, responsibility for access control to the interfaces provided for interoperability would also have to be decided in advance to avoid misuse (spam, unauthorised collection of personal data, etc.).

Table 2: Challenges and potential solutions when implementing interoperability

Challenges	Solutions
Defining the objective and approach of interoperability obligations	Specifying the general interoperability approach (e.g., addressees, functions etc.) and agreement on common technical requirements

⁷⁹ The work within IETF has already started, however, there is no RFC yet and as of September 2022 –the milestone for the first document is expected to be done in September 2022, see <https://datatracker.ietf.org/wg/mls/about/>

⁸⁰ https://mailarchive.ietf.org/arch/msg/mls/B2Pmlor1A9dJ_H2V/VxJM7lus48o/ and <https://datatracker.ietf.org/doc/draft-ietf-mls-architecture/>

⁸¹ https://mailarchive.ietf.org/arch/msg/mls/wlet_qL97hR3Ocr15arMQjXqLpw/ and <https://datatracker.ietf.org/doc/draft-ietf-mls-protocol/>

Challenges	Solutions
Ensuring attractiveness for third party (interoperating) services	Ensuring that core functions are made interoperable in compliance with legal restrictions. Additional functionalities may be made interoperable over time.
Ensuring openness to innovation	Fast process for changing/updating the relevant specifications in keeping with pace of innovation in the industry and to close security gaps quickly
Ensuring data protection and security	Highest possible level of data protection; data protection and data security rules (handling of communication data, user identification, rules on encryption methods, access control rules to prevent misuse)

5.4. Summary of findings

Table 3: Technical comparison of different interoperability approaches for messaging services

	APIs/Interfaces	Bridges	Standardisation
Functions Current Situation: <ul style="list-style-type: none"> • Every provider is free in designing functions and how to implement them • Services may include similar functions, but providers have full freedom which functions they offer. 	<ul style="list-style-type: none"> • Only for specific functions or all functions • Can be adapted quickly 	<ul style="list-style-type: none"> • Only for specific functions or all functions • Bridge needs to be adapted every time APIs are changed 	<ul style="list-style-type: none"> • Functions set in standardisation • Can be adapted only by changing standard
Updates Current Situation: <ul style="list-style-type: none"> • No dependencies for the provider to publish updates, users can get them as fast as the provider offers them 	<ul style="list-style-type: none"> • Process for changing or updating the relevant APIs necessary (e.g., notification of upcoming changes) 	<ul style="list-style-type: none"> • Process for changing or updating the bridge necessary (e.g., notification of upcoming changes) 	<ul style="list-style-type: none"> • Need to be aligned with standardisation process
Innovations Current Situation: <ul style="list-style-type: none"> • Every provider can add new features 	<ul style="list-style-type: none"> • Possible beyond basic functions 	<ul style="list-style-type: none"> • Possible beyond basic functions 	<ul style="list-style-type: none"> • Functions set by the standard • Changes only possible via standardisation

	APIs/Interfaces	Bridges	Standardisation
without coordination			process, this might restrict differentiation and innovation possibilities
Access-requirements Current Situation: <ul style="list-style-type: none"> No access requirement necessary, however providers could introduce interoperability by themselves 	<ul style="list-style-type: none"> No technical requirement for different gatekeepers to use same/similar API Access policies necessary (access to API, usage of data, etc.) 	<ul style="list-style-type: none"> No technical requirement for different gatekeepers to use same/similar bridge Access policies necessary (access to APIs, usage of data, etc.) 	<ul style="list-style-type: none"> Every provider needs to implement the same standard Access requirements and necessary information set by the standard
Development effort Current Situation: <ul style="list-style-type: none"> Every provider carries its own development effort, no agreements with other parties necessary 	<ul style="list-style-type: none"> Existing (proprietary) services can be used, no need to define an entire new standardised framework Effort to develop and maintain API is in the gatekeeper domain However, also access-seekers need to implement API Gatekeeper controls API and necessary information (e.g., identifiers or usage data) 	<ul style="list-style-type: none"> Existing (proprietary) services by the gatekeeper can be used, no need to define an entire new standardised framework Effort to develop and maintain API is in the gatekeeper domain However, also access-seekers need to include bridge in their software Gatekeeper controls API and necessary information (e.g., identifiers or usage data) Bridge provider controls APIs and development of bridge 	<ul style="list-style-type: none"> High development effort due to necessary coordination in standardisation process

	APIs/Interfaces	Bridges	Standardisation
Encryption	<ul style="list-style-type: none"> • In case no common standard for encryption is used, E2EE will be inhibited since contents need to be re-encrypted at the interfaces • If providers can agree on a standard for E2EE, it should work as designed. 	<ul style="list-style-type: none"> • If bridge is provided by third parties, contents need to be re-encrypted (and thus E2EE is not possible) • Only when the gatekeeper itself provides the bridge, E2EE could be possible 	<ul style="list-style-type: none"> • Possible to achieve E2EE in standardisation • Privacy-by-design could be standardised, but potentially high development effort
Privacy	<ul style="list-style-type: none"> • Necessary data is defined by the gatekeeper • Data is exchanged by more parties than before • Also gatekeeper could get access to data from users which use a competing, interoperable service. 	<ul style="list-style-type: none"> • Data is exchanged by more parties than before, also with the bridge provider • Also the bridge provider can potentially access certain data 	<ul style="list-style-type: none"> • Privacy-by-design approach possible via data minimization through standardisation, but potentially high development effort

6. Interoperability of NI-ICS under the DMA

The DMA lays down harmonised rules with the aim of ensuring contestable and fair markets, to the benefit of both business users and end users in the digital sector across the Union where gatekeepers are present.

The DMA applies to core platform services (CPSs) provided or offered by gatekeepers to business users established in the European Union or end users established or located in the Union. In this regard, an overview of these terms (gatekeepers, CPSs) and the conditions for the application of the DMA in these instances is provided below.

For the purposes of this report, a reference to the provisions that deal specifically with interoperability of NI-ICS, as well as those pertaining to governance, is also provided.



6.1. Definition of core platform services and designation of gatekeepers

The DMA contains a list of CPSs. CPSs are services where the presence of a limited number of large online platforms operating as gatekeepers for business users and end-users has led, or will probably lead, to weak contestability of these services and the markets in which they operate. NI-ICS as defined in the EECC, are listed as a CPS.

Likewise, according to the DMA, an undertaking shall be designated as a gatekeeper, if (a) it has a significant impact on the internal market; (b) it provides a CPS which is an important gateway for business users to reach end users; and (c) it enjoys an entrenched and durable position in its operations or it is foreseeable that it will enjoy such a position in the near future. Specifically, an undertaking is presumed to satisfy condition (a) if it meets certain turnover or market capitalisation thresholds which are laid down in the DMA, and (b) provides the same CPS in at least three Member States. For condition (b) to be fulfilled, the CPS must have at least 45 million monthly active end users established or located in the Union, and at least 10 000 yearly active business users established in the Union in the last financial year, as these terms are defined in an Annex to the DMA. Lastly, condition (c) is deemed to be met where the thresholds referred to in condition (b) were met in each of the last three financial years.

When the above criteria are met, the undertaking is to be designated as a gatekeeper by the EC, unless exceptional circumstances duly substantiated are present and justify that the EC does not proceed with the designation. In its designation decision, the EC shall list the relevant CPS that are provided by the undertaking and that individually serve as an important gateway for business users to reach end users.

The EC is also empowered, following a market investigation, to designate an undertaking as a gatekeeper when this undertaking satisfies the general criteria for the designation of gatekeepers referred to above, but does not meet the specific thresholds contained in the DMA and that trigger the presumption that the undertaking is in fact a gatekeeper.

6.2. Interoperability of NI-ICS under the DMA

According to Article 7 of the DMA, designated gatekeepers providing NI-ICS shall make basic functionalities of its NI-ICS interoperable with the NI-ICS of another provider offering or intending to offer such services, by providing the necessary technical interfaces or similar solutions that facilitate interoperability, upon request, and free of charge.

Where the gatekeeper itself provides such functionalities to its own end-users, the following functionalities shall be provided to third parties within the timeframes set out in Article 7:

Table 4: Timeframes for the provision of basic functionalities under the DMA



Within 6 months after the designation	<ul style="list-style-type: none"> (a) end-to-end text messaging between two individual end users; (b) sharing of images, voice messages, videos and other attached files in end-to-end communication between two individual end users. <p><i>[To facilitate the practical implementation of interoperability, a reference offer must be published within six months after the designation decision, and updated where necessary. Once the reference offer has been published, a gatekeeper shall comply with any reasonable interoperability request within three months.]</i></p>
Within two years of the designation	<ul style="list-style-type: none"> (a) end-to-end text messaging within groups of individual end users; (b) sharing of images, voice messages, videos and other attached files in end-to-end communication between a group chat and an individual end user.
Within four years of the designation	<ul style="list-style-type: none"> (a) end-to-end voice calls between two individual end users; (b) end-to-end video calls between two individual end users; (c) end-to-end voice calls between a group chat and an individual end user; (d) end-to-end video calls between a group chat and an individual end user.

The EC is empowered to adopt delegated acts to amend the list of basic functionalities identified above by adding or removing functionalities of NI-ICS. This amending shall be based on a market investigation pursuant to the terms of the DMA, which has identified the need to keep those obligations up to date to address practices that limit the contestability of CPSs or that are unfair. Upon a market investigation, the EC is also empowered to adopt delegated acts to supplement the obligations referred to above by specifying the manner in which those obligations are to be performed in order to ensure effective compliance.⁸²

The DMA requires that the level of security, including end-to-end encryption where applicable, that the gatekeeper provides to its own end users be preserved across the interoperable services. The gatekeeper is also required to publish a reference offer laying down the technical details and general terms and conditions of interoperability with its NI-ICS, including the necessary details on the level of security and end-to-end encryption.

The reference offer shall be published within six months after the designation decision and be updated where necessary. Following the publication of the reference offer, reasonable requests for interoperability with the NI-ICS of the gatekeeper has to be guaranteed within

⁸² The Commission may also adopt implementing acts laying down detailed arrangements for the application of the form, content and other details of the technical measures that gatekeepers shall implement in order to ensure compliance with Article 7; as well as operational and technical arrangements in view of implementing interoperability of NI-ICS pursuant to Article 7.

three months by rendering the requested basic functionalities operational. In any case, the end users of NI-ICS of the gatekeeper and requesting provider shall remain free to decide whether to make use of the interoperable basic functionalities.

Finally, the DMA indicates that the gatekeeper has to collect and exchange with the provider of NI-ICS that requests interoperability only the personal data of the end users that is strictly necessary to provide effective interoperability and in full compliance with the GDPR and e-Privacy Directive. The gatekeeper shall not be prevented from taking proportionate measures to ensure that requests for interoperability by third parties do not endanger the integrity, security and privacy of its services.

6.3. Technical implementation

Regarding the technical implementation, according to Article 46(1)(c) of the DMA, the EC may adopt implementing acts laying down detailed arrangements for the application of operational and technical arrangements in view of implementing interoperability of NI-ICS. Moreover, Article 48 and Recital 96 DMA mention that interoperability obligations could be facilitated by the use of technical standards and that, where appropriate and necessary, the EC may request European standardisation bodies to develop them.

As the definition of interoperability in Article 2 (29) of the DMA includes the exchange and use of information “*which has been exchanged through interfaces or other solutions*”, the DMA does not make any further concrete specifications as to which technical interoperability approach is to be chosen. For this reason, the above-mentioned interoperability approaches are conceivable in principle. However, some of these approaches may be preferable for certain contexts. For instance, given that the requirements described above (such as the same level of security) need to be implemented, bridges might not be able to meet all requirements (such as end-to-end encryption).

The gatekeeper is required to publish the technical details and general terms and conditions of interoperability with its NI-ICS in a reference offer. BEREC and National Regulatory Authorities (NRAs) already have many years of experience with reference offers.⁸³ In electronic communications markets, regulated wholesale offers are a common instrument to promote transparency and prevent discriminatory terms. With regard to the specific challenges identified in implementing interoperability in chapter 5.3, minimum requirements for an interoperability reference offer could include:

- **description of the service and specification of the relevant basic functionalities and their features/facilities;**

⁸³ Ibid footnote 7

- **technical definition and documentation of relevant interfaces and standards** to be used (e.g., communications protocols, API descriptions), including any technical usage restrictions;
- **data protection rules** (handling, use and storage of communication (meta)data, user identification);
- **data security rules** (level of security and encryption methods, especially end-to-end encryption, key management etc.);
- rules on **dynamic adjustments** (technical updates for basic functionalities, dealing with security incidents, announcement of updates, migration path etc.);
- rules on **dispute resolution** between providers including support handling;
- **access control rules** to prevent misuse;
- Details on necessary interoperability tests;
- **Service level agreements and service level guarantees** (e.g. on availability);
- **Key performance indicators** including threshold values;
- Relevant charges (penalties), terms of payment⁸⁴ and billing procedures;
- Rules regarding the **implementation of obtaining users' consent** to use the interoperable basic functions (e.g... concept and design of an opt-in process to obtain informed user consent);
- Details of duration, renegotiation and causes of termination of agreements as well as other associated contractual terms;
- Definition and limitation of liability and indemnity;
- Relevant information relating to a **single point of contact** at the **gatekeeper** for requesting and implementing interoperability for providers of NI-ICS offering or intending to offer such services in the Union.

Concerning technical implementation, it is finally worth recalling that Recital 64 DMA states that it should be possible for the EC, if applicable, to consult BEREC in order to determine whether the technical details and the general terms and conditions, published in the reference offer which the gatekeeper intends to implement or has implemented, ensure compliance with the interoperability obligation.

⁸⁴ It should in any event be recalled that, on the basis of article 7 of the DMA, interoperability should be provided free of charge. This does not exclude that the gatekeeper might propose other functionalities on top of the basic features on a commercial basis, which may be subject to specific terms of payment.

6.4. Governance

According to the DMA, the EC is the sole authority empowered to enforce the provisions contained therein. The DMA however foresees different cooperation mechanisms, in particular with the competent authorities of the Member States enforcing competition rules.

Moreover, the DMA foresees the establishment of a High-Level Group which includes BEREC⁸⁵. The High-Level Group is to have a secretariat, to be provided by the EC, which will also chair the group and participate in the meetings. The High-Level Group must meet upon request of the EC at least once per calendar year. The EC has to also convene a meeting of the group when so requested by the majority of the members composing the group in order to address a specific issue.

Regarding its tasks, the High-Level Group has to provide the EC with advice and expertise in the areas falling within the competences of its members⁸⁶. In particular, concerning interoperability for NI-ICS, BEREC's contribution may focus on providing advice and recommendations for the implementation and enforcement of this measure, as well as expertise for promoting a consistent regulatory approach across different regulatory instruments (e.g., the EECC)⁸⁷.

Moreover, within the High-Level Group, BEREC will also be able to provide expertise to the EC on the need to modify, add or remove rules of the DMA, to ensure that digital markets across the Union are contestable and fair.

7. Interoperability of NI-ICS under the EECC

7.1. NI-ICS in the ECS regulatory framework

The EECC contains certain obligations that apply to all types of ICS. NI-ICS are however subject to a more limited range of obligations than NB-ICS, on the basis that the latter participate, and hence also benefit from, a publicly assured interoperable ecosystem.⁸⁸

Regarding the applicable obligations, NI-ICS must provide NRAs, other competent authorities (OCAs) and BEREC with the information that may be necessary for the fulfilment of their tasks (Article 20 EECC). Given that NI-ICS are a type of ECS, the provisions on dispute resolution

⁸⁵ Together with four other European networks/bodies: the European Data Protection Supervisor and European Data Protection Board; the European Competition Network; the Consumer Protection Cooperation Network; and the European Regulatory Group of Audiovisual Media Regulators.

⁸⁶ Article 40, Ibid footnote 1.

⁸⁷ This can imply the preparation of an annual report to the Commission to identify potential trans-regulatory issues. The annual report may be accompanied by recommendations aiming at converging towards consistent transdisciplinary approaches and synergies between the implementation of the DMA and other sectoral regulations.

⁸⁸ Recital (18) of the EECC, Ibid footnote 2.

in the EECC, both at the retail and wholesale levels, apply to this category of players (Articles 25 and 26 EECC). The EECC provisions pertaining to end-user rights also apply to a large extent to NI-ICS.⁸⁹

As it will be detailed in the sections below, obligations for interoperability of NI-ICS are set out in particular in Article 61(2) EECC. For the purposes of analysing the interoperability measures set out in the EECC, a brief reference to the legal framework applicable to security, privacy and standardisation issues may also be illustrative.⁹⁰

First, NI-ICS are subject to the provisions of the EECC, as well as Article 4 of the ePrivacy Directive⁹¹, which deal respectively with the security of networks and services and security of processing⁹². As of 21 December 2020, by virtue of the EECC definitions, the ePrivacy Directive applies to all ECS, including NI-ICS.⁹³

On the basis of the EECC, NI-ICS must take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of the services being provided⁹⁴. These measures are to ensure a level of security appropriate to the risk presented. This includes measures to prevent and minimise the impact of security incidents on users and on other networks and services (including encryption where appropriate).

On the other hand, and in addition to the above, technical and organizational measures adopted under the ePrivacy Directive have to at least:

- ensure that personal data can be accessed only by authorized personnel for legally authorized purposes,

⁸⁹ Ibid footnote 6 for further insights on the EECC definitions of the services and a detailed description of the EECC rules that apply to NI-ICS.

⁹⁰ As also referred to in Chapter 5.3 of the report.

⁹¹ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p.37), amended by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, L 105,54,13.4.2006 and Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219>

⁹² The e-Privacy Directive is currently under review by means of a proposal for a Regulation on Privacy and Electronic Communications,

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN>

⁹³ This was clarified in Regulation (EU) 2021/1232 of the European parliament and of the Council. See <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R1232>, and in

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN>

⁹⁴ Article 40 EECC. Recital (95) of the EECC notes that, given that providers of NI-ICS services normally do not exercise actual control over the transmission of signals over networks, the degree of risk for such services can be considered to be lower than for traditional electronic communications services. Therefore, where justified on the basis of the actual assessment of the security risks involved, the measures taken by providers of NI-ICS may be lighter than those taken by other ECS providers.

- protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorized or unlawful storage, processing, access or disclosure and,
- ensure the implementation of a security policy with respect to the processing of personal data.

Second, regarding protection of privacy in the electronic communications sector, the European personal data protection regime also applies to NI-ICS, under the terms and conditions provided therein. The cornerstone of personal data protection in the EU is the General Data Protection Regulation (GDPR)⁹⁵, which lays down the general rules relating to the protection of natural persons with regard to the processing of personal data and the free movement of personal data.

The ePrivacy rules, which as noted above apply to ECS (including NI-ICS), protect the confidentiality of electronic communications data of both natural and legal persons. The general rule established in Article 5 of the e-Privacy Directive is that electronic communications data shall be confidential. Any interference with electronic communications data, including listening, tapping, storing or other kinds of interception or surveillance of electronic communications data, without the consent of the users concerned, is prohibited except when legally authorised to do so. Furthermore, storing of information or gaining of access to information stored in the terminal equipment is only allowed with the consent of the user or subscriber concerned unless the aim of the technical storage or access is limited to carrying out the transmission or the provision of an information society service explicitly requested by the subscriber or user.

Finally, although the EECC acknowledges that standardisation should remain primarily a market-driven process⁹⁶, it also foresees situations where it may be appropriate to require compliance with specified standards at Union level to improve interoperability, freedom of choice for users and encourage interconnectivity in the internal market.

In this regard, Article 39 EECC provides that the EC may request (and Member States may encourage) that standards be drawn up to ensure interoperability of services and end-to-end connectivity, among other aims.

In the case that existing standards have not been adequately implemented so that interoperability of services in one or more Member States cannot be ensured, the EC, by means of implementing acts, can make the implementation of such standards or specifications

⁹⁵ Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016.

<https://eur-lex.europa.eu/eli/reg/2016/679/oj> <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

⁹⁶ Recital (93) of the EECC, Ibid footnote 2



compulsory to the extent strictly necessary to ensure such interoperability and to improve freedom of choice for users.

7.2. Article 61(2) EEECC

Article 61 EEECC regulates access, interconnection and interoperability for ECNs and ECSs, including both NB-ICS and NI-ICS.

In the case of NI-ICS, under Article 61(2)(c) EEECC, NRAs or OCAs shall be able to impose, *“where end-to-end connectivity between end-users is endangered due to a lack of interoperability between interpersonal communications services, and to the extent necessary to ensure end-to-end connectivity between end-users, obligations on relevant providers of number-independent interpersonal communications services which reach a significant level of coverage and user uptake, to make their services interoperable”*.

This means that, in cases where end-to-end connectivity is endangered, interoperability obligations may be imposed in justified cases *only* on NI-ICS that have a significant level of coverage and user uptake. Moreover, Article 61 sets out two conditions in view of the imposition of interoperability obligations on NI-ICS:

- The obligations must be limited to the extent necessary to ensure interoperability of NI-ICS and may include proportionate obligations on providers of those services to publish and allow the use, modification and redistribution of relevant information by the authorities and other providers, or to use and implement standards or specifications listed in Article 39 (1) or of any other relevant European or international standards; and
- the EC, after consulting BEREC and taking utmost account of its opinion, must have found an appreciable threat to end-to-end connectivity between end-users throughout the EU or in at least three Member States and has adopted implementing measures specifying the nature and scope of any obligations that may be imposed.

It is thus apparent that Article 61(2)(c) should be understood as a measure of last resort, to be applied in exceptional circumstances.

7.2.1. Procedure for imposing interoperability on NI-ICS

The identification and assessment of interoperability issues that may require regulatory intervention is done by the EC, BEREC and the NRA/OCA at different stages. As described in Recital 150 EEECC, when an interoperability issue arises with regard to NI-ICS, the EC would request a BEREC report assessing the market situation at the EU and national level. In view of this report, the EC may consider that there is a need for regulatory intervention and adopt implementing measures specifying the nature and scope of possible regulatory intervention, including obligations to publish and allow the use, modification and redistribution of relevant

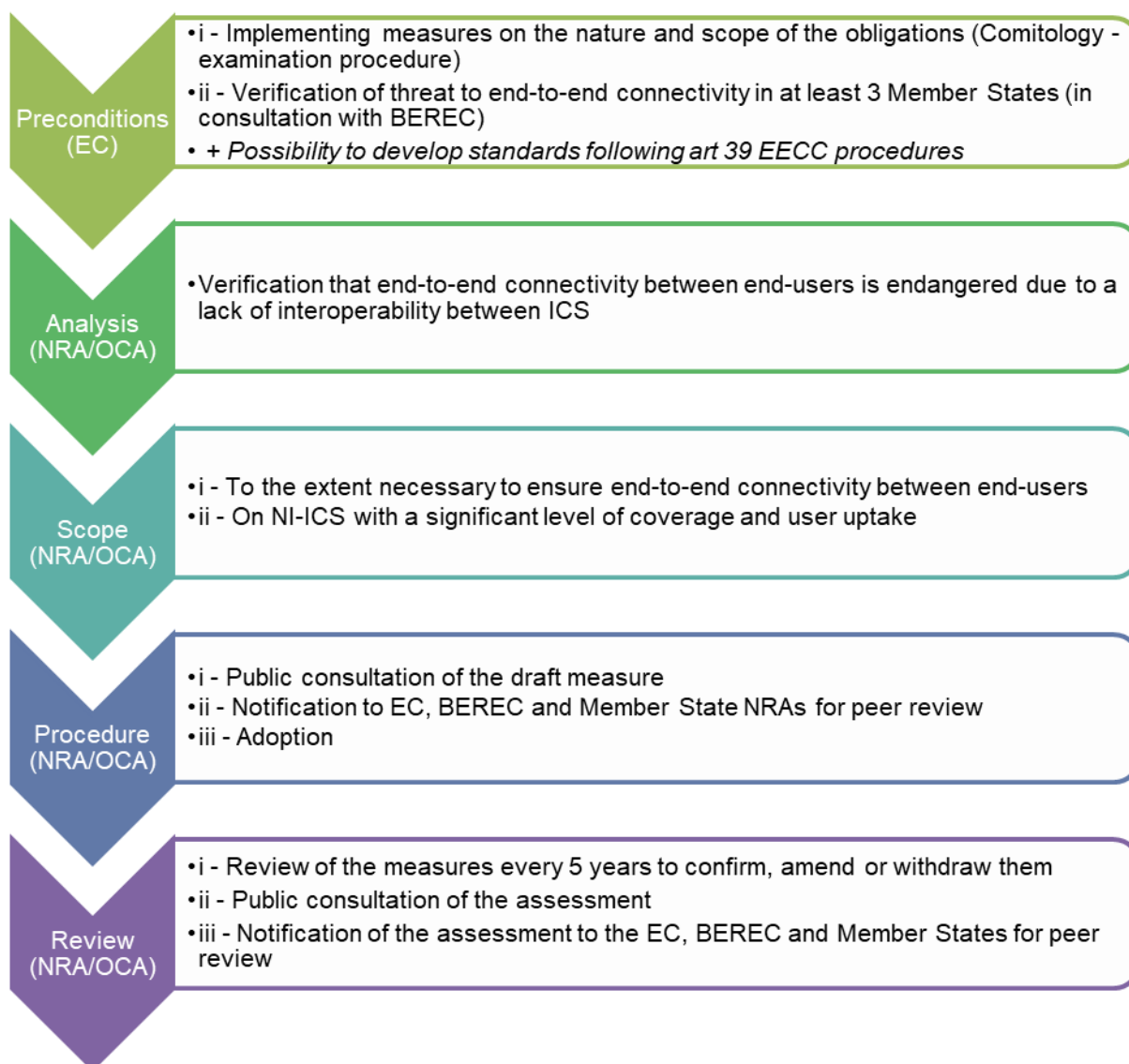
information by the authorities and other providers and measures to impose the mandatory use of standards or specifications on all or specific providers.

That is, even though the competence to impose the obligation lies within national authorities, the initiative to allow NRAs/OCAs to adopt such decisions is under the EC remit and is subject to the EC implementing measures to ensure that the obligation imposed on NI-ICS is coherent across the EU. In addition, NRA/OCA's draft measures in application of Article 61(2) EECC are subject to the procedures under Article 23 (public consultation) and Articles 32 and 33 EECC (notification to the EC and peer review by BEREC and the other NRAs). The results of imposing such obligations shall be reviewed by the NRA/OCA every 5 years.

It is also worth mentioning the important role that European standardisation organisations may play in this context, as the standards or specifications whose use or implementation may be required by NRA/OCAs shall be those referred to in Article 39(1) of the EECC, or any other relevant European or international standards.

Figure 6: Article 61(2) step-by-step procedure





7.2.2. Conditions for imposing interoperability on NI-ICS

The EECC considers interoperability to be an important objective of the regulatory framework to be pursued by NRAs and OCAs, for the benefit of end-users⁹⁷. The EECC approach to interoperability, however, significantly differs between NB-ICS and NI-ICS.

In particular, NI-ICS are not, in principle, obliged by the EECC to make their services interoperable. However, such an obligation can be imposed when end-to-end connectivity between end-users is endangered due to a lack of sufficient interoperability, and only on NI-ICS with a significant level of coverage and user uptake.

⁹⁷ Recital (148) of the EECC, Ibid footnote 2

7.2.2.1. When can end-to-end connectivity between end-users be considered endangered?

As previously described, the analysis of the risk to interoperability is undertaken first by the EC, then by the NRA/OCA and, finally, reviewed by the EC, BEREC and peer NRAs.

Recital (149) EECC notes that *“currently both end-to-end connectivity and access to emergency services depend on end-users using number-based interpersonal communications services. Future technological developments or an increased use of number-independent interpersonal communications services could entail a lack of sufficient interoperability between communications services. As a consequence, significant barriers to market entry and obstacles to further onward innovation could emerge and appreciably threaten effective end-to-end connectivity between end-users”*.

The baseline as highlighted in the recitals of the EECC is that end-to-end connectivity and access to emergency services are, to date, ensured by NB-ICS. In a scenario where, for instance, users do not opt to avail of NB-ICS, end-to-end connectivity might no longer be ensured, and regulatory intervention may be needed to restore it. In this regard, in the case of NB-ICS (voice telephony, SMS, MMS) the end-to-end connectivity concept is clear: it describes the process of enabling users to make calls or send messages to other users on the same network or on other providers' networks via the use of numbers in national or international numbering plans. Competing communications providers need to be able to interconnect with other networks to provide a full (competitively viable) service to their customers. Customers expect to be able to call and send messages to every other retail customer irrespective of the network to which the called party is connected. As noted, the EECC considers that end-to-end connectivity is for the time being ensured by end-users making use of NB-ICS.

Regarding NI-ICS, in particular messaging services, they have typically been based on proprietary protocols and are therefore not interoperable with each other. Thus, the choice of provider matters, as one user can only interact with other users of the same messaging service⁹⁸. Furthermore, by contrast with NB-ICS, the array of functionalities associated with messaging services is broader and may vary from one service to another. This raises the question of what functionalities should be considered when assessing the impact, if any, on end-to-end connectivity.

The EECC assumes in Recital (149) that end-to-end connectivity between users might be indirectly threatened by technological developments and an increased use of NI-ICS that are not sufficiently interoperable. There is therefore a clear connection between “sufficient” interoperability and end-to-end connectivity on the one hand, and a perceived risk to end-to-end connectivity if such increased uptake of NI-ICS is coupled with a corresponding decline of access to and take-up of NB-ICS.

⁹⁸ Ibid footnote 23

To sum up, regarding end-to-end connectivity, the EECC specifically highlights two factors that are relevant to ascertain whether end-to-end connectivity between users may be endangered:

- First, it should be verified whether interoperability is still “sufficient” in the light of technological developments and/or an increased use of NI-ICS;
- Second, in that context, it should be assessed whether the role played by NB-ICS in ensuring end-to-end connectivity (as well as access to emergency services) is diminished or undermined by such developments and/or the increased use of NI-ICS.⁹⁹

In addition to these two factors, and to preserve its future-proof approach, the assessment of end-to-end connectivity endangerment may include other factors, such as the role of multi-homing on NI-ICS.

In this respect, end-to-end connectivity, as a principle derived from traditional electronic communications regulation, might not be directly transferrable to NI-ICS, as each of these services fulfils various individual needs of users. In this line, Kerber and Schweitzer (2017)¹⁰⁰ note that users effectively ensure end-to-end connectivity by multi-homing across various NI-ICS. This is straightforward in case the user is willing to substitute or multi-home across multiple NI-ICS to use specific functionalities (group chat, high resolution video, etc.). In the absence of a bottleneck, due to multi-homing for instance, end-to-end connectivity issues may thus not be as prevalent¹⁰¹. This also raises the question of whether ‘end-to-end connectivity’ is interpreted (and therefore expected) by users in a similar manner for services that are number-based (NB-ICS), as opposed to those that are provided independently of the number-based system (NI-ICS). It could be the case that users expect ‘full’ end-to-end connectivity where the service is number-based, whereas for services that are number-independent, the expectation may be that they can increase the extent of connectivity to other users simply by multi-homing, a practice which users likely consider easy and generally free of monetary charge (unlike the case of NB-ICS). This intuition would in any event have to be tested by NRAs in practice, by looking at factors such as usage or the widespread availability of the alternatives to which users could resort to, as highlighted in chapter 4 of the report.

⁹⁹ This may lead to assessing substitutability trends between NB-ICS and NI-ICS, as well as traffic trends between both categories of services.

¹⁰⁰ Ibid footnote 51, p. 39–58.

¹⁰¹ See, in the context of an analysis of article 5 of the former Access Directive, BoR (12) 130, BEREC Report: An assessment of IP interconnection in the context of Net Neutrality, 06.12.2012.

<https://www.berec.europa.eu/en/document-categories/berec/reports/an-assessment-of-ip-interconnection-in-the-context-of-net-neutrality> <https://www.berec.europa.eu/en/document-categories/berec/reports/an-assessment-of-ip-interconnection-in-the-context-of-net-neutrality>

7.2.2.2. When can the level of coverage and user uptake of a NI-ICS be considered significant?

The EECC states that, in case they are deemed necessary, interoperability obligations should only be imposed on NI-ICS which reach a significant level of coverage and user uptake. According to Recital 151 EECC, *“the term significant should be interpreted in the sense that the geographic coverage and the number of end-users of the provider concerned represent a critical mass with a view to achieving the goal of ensuring end-to-end connectivity between end-users. Providers with a limited number of end-users or limited geographic coverage which would contribute only marginally to achieving that goal, should normally not be subject to such interoperability obligations”*.

The imposition of interoperability on NI-ICS under Article 61(2) EECC is not, therefore, directly related to the NI-ICS market power, but focused on the need to reach a critical mass of users with a view to achieving end-to-end connectivity.

NI-ICS interoperability obligations are in any event not symmetric in nature (that is, they do not apply across-the-board to all NI-ICS providers) but rather asymmetric, in that only some providers of NI-ICS services may be subject to such measures. Keeping this in mind, Article 61(2) EECC is sufficiently broad to include within its remit different NI-ICS, for as long as they all reach a significant level of coverage and user uptake and are found to appreciably endanger end-to-end connectivity.

Although the identification of the affected NI-ICS providers is theoretically separate and subsequent to the assessment of end-to-end connectivity endangerment, in practice, considering the inherent features of these services such as network effects, it is most likely that the analysis of the end-to-end connectivity endangerment would also entail the identification of the key provider(s) of NI-ICS. In this respect, using turnover might not, *by itself*, be a good tool for verifying whether a specific NI-ICS reaches a particular level of coverage and user uptake, also taking into account that many of the services are provided “free of charge”¹⁰². In the DMA, the references to turnover in view of the designation of gatekeepers are understood to act as a proxy of whether the gatekeeper has a significant impact on the internal market, which is different from the requirement set in the EECC that the specific level of coverage and user uptake of NI-ICS be assessed.

The number of monthly/yearly active end-users might on the other hand be a more useful proxy. It is in any event worth mentioning that the figures provided in the DMA should not be automatically incorporated into the Article 61(2) assessment, considering the EU dimension of the DMA (as opposed to the analysis that NRA/OCAs will need to undertake at national

¹⁰² As noted throughout the report, “free of charge” meaning with no explicit monetary cost, but without prejudice to the different ways NI-ICS have to monetize the use that is being made of the service.

level under the EECC) as well as the different objectives and instruments contained in both sets of legislation¹⁰³.

Other parameters that might be relevant for the purposes of evaluating whether the level of coverage and user uptake is “significant” may include the availability (or not) of the NI-ICS; the appeal of the NI-ICS to end-users; or related parameters that may enable the provider to benefit from possible scale, scope and network effects. Another valuable insight, for national scale assessments, could be the size and direction of difference between the combined number of NB-ICS subscribers (of all providers) and the monthly/daily active users of the (largest) NI-ICS under review. In scenarios where there are more users of this NI-ICS than there are combined subscribers of NB-ICS, it could be argued that end-to-end connectivity may be more easily satisfied, in that territory, via this specific NI-ICS. This however would also require an assessment of the extent at which connectivity is possible, for instance, if it would also entail access to emergency services.¹⁰⁴

These features have been analysed in more detail in chapter 4.

8. Interplay between the DMA and the EECC

Article 61(2) EECC shares common features with Article 7 DMA, the primary purpose of both provisions being to ensure interoperability of NI-ICS. The EECC and the DMA differ however in the way interoperability obligations can be set, and in some important procedural aspects. These elements are summarised in the table below.

Table 5: Comparison of Article 61 (2) EECC and Article 7 DMA

Article 61 (2) EECC		Article 7 DMA
Designated NI-ICS	Key providers of NI-ICS which reach a significant level of coverage and user uptake.	Designation of gatekeepers providing CPSs (incl. NI-ICS) is presumed when the specific thresholds provided for in Article 3 of the DMA are met. Exceptions may however apply on the basis of the procedure set in the DMA (and likewise, a gatekeeper may be designated

¹⁰³ In this regard, the purpose of the DMA is to contribute to the proper functioning of the internal market by laying down harmonised rules ensuring contestable and fair markets to the benefit of both business users and end-users in the digital sector across the Union (as set in Article 1.1) Ibid footnote 1

¹⁰⁴ For BEREC analysis on these aspects, see BEREC Opinion on the market and technological developments and on their impact on the application of rights of end-users in the EECC. BoR (21) 177. 15.12.2022. <https://www.berec.europa.eu/en/document-categories/berec/opinions/berec-opinion-on-the-market-and-technological-developments-and-on-their-impact-on-the-application-of-rights-of-end-users-in-the-eecc>

Article 61 (2) EECC		Article 7 DMA
		even if the specific thresholds foreseen in the DMA are not met ¹⁰⁵).
Substantive provisions: triggering event	When end-to-end connectivity between users is endangered due to a lack of interoperability between interpersonal communications services, and to the extent necessary to ensure end-to-end connectivity between users.	<p>Designation by the EC of the undertaking as a gatekeeper which provides NI-ICS that are listed in the designation decision.</p> <p>The initial interoperability requirement applies to (i) end-to-end text messaging between two individual end users; (ii) sharing of images, voice messages, videos and other attached files in end-to-end communications between two individual end users.</p> <p>Additional functionalities to be made interoperable within two and four years of the designation as a gatekeeper.</p>
Substantive provisions: scope of the obligations and significant implementation requirements	Obligations may only be imposed (i) to the extent necessary to ensure interoperability of interpersonal communications services, which may include proportionate obligations on providers of those services to publish and allow the use, modification and redistribution of relevant information by the authorities and other providers, or to use and implement standards or specifications listed in Article 39(1) EECC or of any other relevant European or international standards; and (ii) where the EC, after consulting BEREC and taking utmost account of its opinion, has found an appreciable threat to end-to-end connectivity between end-users throughout the Union or in at least	<p>Gatekeepers providing NI-ICS shall make basic functionalities of its NI-ICS interoperable with the NI-ICS of another provider offering or intending to offer such services, by providing the necessary technical interfaces or similar solutions that facilitate interoperability, upon request, and free of charge.</p> <p>The level of security, including end-to-end encryption where applicable, that the gatekeeper provides to its own end users shall be preserved across the interoperable services.</p> <p>The end-users of the gatekeeper and requesting</p>

¹⁰⁵ Article 3(8) DMA Ibid footnote 1

	Article 61 (2) EECC	Article 7 DMA
	three Member States and has adopted implementing measures specifying the nature and scope of any obligations that may be imposed.	provider shall remain free to decide whether to make use of the interoperable basic functionalities that may have been provided.
Procedure	Two-step procedure: (i) EC adopts implementing measures on the nature and scope of the obligations; (ii) NRAs/OCAs impose obligations on relevant providers of NI-ICS which reach a significant level of coverage and user uptake.	<p>Gatekeeper to publish within six months a reference offer laying down the technical details and general terms and conditions of interoperability with its NI-ICS.</p> <p>Following the publication of the reference offer, interoperability with the NI-ICS must be ensured within three months upon receipt of a request.</p> <p>The EC may consult BEREC to determine whether the reference offer ensures compliance with the obligation of NI-ICS interoperability.</p>
Governance	EC; BEREC; NRAs/OCAs.	EC as the sole authority empowered to enforce DMA. The EC can consult BEREC on the reference offer proposed by the gatekeeper. Cooperation mechanisms are foreseen, including with the high-level group which includes BEREC amongst its members.

As it can be seen from the table above, the DMA and the EECC share a similar scope (both deal with interoperability of NI-ICS), but pursue different objectives¹⁰⁶, and work differently. The provisions of the DMA are to a certain extent *ex ante* in their nature, in that they will automatically apply (as SMP obligations do) once a designation decision is adopted by the EC. On the other hand, the provisions of the EECC act as a regulatory response to trends

¹⁰⁶ While Article 61(2) aims to protect end to end connectivity when endangered, interoperability in the context of Article 7 of the DMA aims at reducing the barriers to entry and fostering the contestability of NI-ICS.

witnessed in the market, which may lead to end-to-end connectivity being endangered due to a lack of interoperability between ICS.

The coherence between the DMA and the EECC should in any event be ensured through the governance structures that are set in both instruments. First, in both instances the EC assumes a leading role, be it directly as the institution in charge of adopting the designation decision and monitoring compliance with the obligations (DMA) or through the enactment of implementing measures specifying the nature and scope of the obligations that NRAs can impose (EECC). Likewise, the participation of BEREC in the high-level group, and in the revision of the reference offers elaborated by gatekeepers (if consulted by the EC), should foster consistency between both types of instruments.

In this context, for the NI-ICS that will be subject to the DMA obligation, any further action on the basis of Article 61(2) EECC will likely depend on the success and evolution of the measures initially envisaged under the DMA. There might however be some instances where further action could be envisaged in the future. This might for instance be the case if for whichever reason alternative operators do not make use of the interoperability functionalities offered by the designated gatekeeper(s), and/or if it is deemed necessary to extend interoperability, under the EECC, to other key ICS providers different from gatekeepers which also reach a significant level of coverage and user uptake¹⁰⁷.

The future reach of the EECC might also be dependent upon the specific categories of NI-ICS provided by the gatekeepers that are finally covered by the designation process enshrined in the DMA. As it has been noted, different categories of services may fall within the notion of NI-ICS, so it will have to be seen what the precise remit of the DMA is, in order to ascertain the scope for further action under the EECC for other types of NI-ICS that might not be initially covered by the DMA. Also, the notion of NI-ICS is dynamic and might evolve over time, a feature that will have an impact on the way the DMA and the EECC apply.

9. Conclusions

NI-ICS typically include messaging, video-conferencing and e-mail services. Their use has drastically increased in the last decade and such services have now become a crucial means of communication for a variety of different users throughout Europe.

Chapters 3 and 4 showed how the features of messaging services (e.g. very strong network effects, consumer inertia, etc.) result in significantly concentrated markets. While multi-homing is possible and common, users mainly rely on a small number of applications, all belonging to a very limited number of players.

¹⁰⁷ As noted, the conditions for the designation of an undertaking as a gatekeeper under the DMA are different from the conditions for intervention laid down in article 61(2) EECC.



Interoperability obligations for specific NI-ICS providers are included under Article 7 DMA and Article 61(2) EECC.

Chapter 5 detailed the different technical approaches to apply interoperability measures and the implementation challenges which should be taken into account. In particular, the different technical implementation options (e.g., APIs or bridges provided by the NI-ICS provider, or through a standardisation process) all have advantages and disadvantages that need to be considered and balanced. Regardless of the chosen approach, BEREC believes that it is crucial to include an appropriate updating mechanism, allowing for adding new functions, quickly closing security gaps and, at the same time, enabling all market participants to be informed in due time about future changes.

BEREC also provided a first list of minimum criteria to be included in the reference offer that the gatekeeper have to prepare under the DMA. Such aspects include service level agreements and guarantees, key performance indicators including threshold values, as well as other relevant technical information.

Chapters 6 and 7 presented the objectives, the scope and the “triggers” of interoperability obligations under both the DMA and the EECC, and BEREC’s insights on the interplay between the two frameworks is highlighted in Chapter 8. In general, BEREC believes that the interoperability provisions under the DMA and the EECC share a similar objective, but work in a different, complementary way, and that the coherence between two regulatory frameworks must be ensured through the respective governance structures (i.e. leading role of the EC and active involvement of BEREC).

This report mainly focuses on messaging services, but BEREC may further work on the interoperability of other NI-ICS, such as video-conferencing services.

BEREC would like to stress again its willingness to further cooperate with the EC on the implementation of the DMA, and remains at their disposal to determine whether the technical details and the general terms and conditions published in the gatekeeper’s reference offer ensures compliance with the interoperability obligation in the DMA. Moreover, BEREC will actively contribute to the DMA High-Level Group providing advice and expertise relevant to the implementation and enforcement of the DMA.

10. Future work

In order to ensure early and timely input to the EC for the enforcement of the DMA, the present report is mainly focused on messaging services. However, BEREC recognises the relevance of analysing interoperability measures for other types of NI-ICS, such as videoconferencing services.

When it comes to email services, interoperability is already in place and based on standardised formats and protocols (e.g., SMTP, IMAP). This does not mean that there may

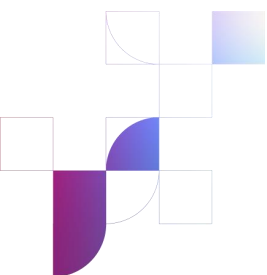


not be potential issues concerning effective interoperability and in a broader, but related scope migration and switching. For instance, some constraints may be imposed by the providers for security or spam-protection reasons, *de facto* limiting server-to-server communications. These aspects may be further explored in the future by BEREC.

The provisions concerning NI-ICS interoperability under the DMA include the possibility for the EC to consult BEREC in order to determine whether the technical details and the general terms and conditions published in the reference offer that the gatekeeper intends to implement or has implemented ensures compliance with the interoperability obligation (Recital 64 DMA). BEREC stresses its willingness to further cooperate with the EC to ensure an effective implementation of the DMA.

Furthermore, the DMA also provides for the set-up of a High-Level Group (Article 40 DMA) which brings together five European networks and bodies, including BEREC. BEREC has already started discussions with the EC in order to ensure an effective contribution to this Group and an application of the DMA which is consistent with other regulatory frameworks in force.

Finally, as a related topic, BEREC will keep analysing the practices of the main digital actors and the services they offer. In particular, BEREC will focus on the entry of large content and application providers (CAPs) into the markets for ECNs and ECSs in 2023. To this end, BEREC will identify the elements in which large CAPs have been increasingly investing and their strategies to move upwards along the value chain. It will also depict the dynamics of competition and/or of cooperation between ECN/ECS providers and these companies, and will analyse both new services and new business models and strategies implemented by these actors.



ANNEX 1: List of abbreviations

API	Application Programming Interface
CPS	Core Platform Service
BEREC	Body of European Regulators for Electronic Communications
DMA	Digital Markets Act
EC	European Commission
ECN	Electronic Communications Network
ECS	Electronic Communications Services
EECC	European Electronic Communications Code
ICS	Interpersonal Communication Services
NI-ICS	Number-Independent Interpersonal Communication Services
NB-ICS	Number-Based Interpersonal Communications Services
NRA	National Regulatory Authorities
OCA	Other Competent Authorities
SMP	Significant Market Power
SMS	Short Message Service



ANNEX 2: List of figures and tables

Table 1: Comparison of different types of services in terms of features..... 8

Table 2: Challenges and potential solutions when implementing interoperability 25

Table 3: Technical comparison of different interoperability approaches for messaging services
..... 26

Table 4: Timeframes for the provision of basic functionalities under the DMA 29

Table 5: Comparison of Article 61 (2) EECC and Article 7 DMA..... 42

Figure 1: The main applications identified by European end-users for interpersonal communications, Analysing EU consumer perceptions and behaviour on digital platforms for communication, PPMI, 2020 data..... 12

Figure 2: Regular use of multiple messenger applications..... 14

Figure 3: Application Programming Interfaces..... 18

Figure 4: Bridge 19

Figure 5: Standardisation 21

Figure 6: Article 61(2) step-by-step procedure 37

