Internet
made in France

Registrars' and Users' Consultative Committee meetings

Minutes of 26 November 2025

Contents

1. Attendees

Users

10 persons representing 12 members of the college.

- BACHOLLET Sébastien, representing ISOC France
- BEAUVILLAIN Caroline, representing INPI
- BOUTIGNON Antoine
- CHELLY David
- JOLY-BACHOLLET Anne-Marie
- LOUIS Benjamin, representing SPARKLING
- MELLET Marc-Emmanuel, representing NOVAGRAAF
- NGUYEN François
- PAWLAK Nicolas
- TAYER David-Irving

Registrars

19 persons representing 18 members of the college.

- ALMIRON Sébastien, representing NETIM
- BERNARD Marc-Olivier, representing TERADOC
- CANER Emma, representing OVH Cloud
- CHUNG Lie Sue, representing NAMESHIELD
- DESSENS Emilie, representing DOMAINOO
- DE NICOLAY Ludovic, representing VIADUC

- DULAC Bernard, representing DATAXY
- FRANCK Philippe, representing DOMAINIUM
- FRANQUINET Arnaud, representing GANDI
- HAUSS Patrick, representing CSC
- HUGLA Alexandre, representing SCALEWAY
- GEOFFROY Pierre, representing ONE2NET
- JEAN-GILLES Sophie, representing ORANGE
- KORN Jennifer, representing ORDIPAT
- LANTONNET Eric, representing DIGITAL GROUP SERVICES
- LEROY Cédric, representing SCALEWAY
- MANCEC Gael, representing CABINET GERMAIN MAUREAU
- SEUFER Luc, representing EuroDNS
- WITTERSHEIM Arnaud, representing NAMESHIELD

Afnic

- AMPEAU Benoît, Partnerships and Innovations Director
- BELLIARD Elodie, Head of Customer Relations
- BONIS Pierre, CEO
- CANAC Sophie, Head of Associative Governance
- CAPLAIN Linda, Head of Quality and Registry Services Improvement
- DAMILAVILLE Loic, Survey and Market Intelligence Manager
- GEORGELIN Marianne, Legal Director, Head of Registry Policy & Public Affairs
- MASSÉ Régis, Director of Information Systems
- PASSEREAU Mégane, Assistant to General Management
- PESQUER Maelle, Events Communication Manager
- TURBAT Emilie, Marketing and Commercial Director
- VAN DER WAL Marc, R&D Engineer

2. Agenda

Welcome and news update

Information update and discussion items:

- Registrars' adoption of APIs
- Afnic's proposals in response to State RFPs for the concession of management of the French overseas TLDs and information on changes to the Naming Policy
- NIS 2
- Study of the V2 renewal rate
- Points raised by members

Subjects submitted for consultation

- Implementation of two-factor authentication (2FA) for connections to Afnic's extranets
- Improvement of technical and operational documentation and operational communication
- Detection of registration data contrary to the Naming Policy immediately upon creation of the domain name: extension and development of the system
- Improved detection of abuse thanks to machine learning

Separate committee meetings

Feedback from the separate committee discussions and Afnic's responses

Calendar of upcoming Afnic diary dates

3. Welcome & news update

Pierre Bonis welcomed the participants, including those joining the meeting remotely.

Pierre Bonis and the co-chairs thanked the members for their attendance. In agreement with the chairs of the committees and on an exceptional basis, the order of the agenda items was reversed for reasons of convenience.

NEWS UPDATE

The annual general meeting of ICANN, the Internet Corporation for Assigned Names and Numbers, which was held this year in Dublin, attracted a large number of French domain name actors who were also Afnic members. The event confirmed the increasingly technical positioning of ICANN, a development that is not without significance in the context of the discussions around stocktaking of the World Summit on the Information Society and the advent of the multi-stakeholder model. Its Board of Directors adopted the Applicant Guidebook, with pointers for candidacies for the new gTLD round. Afnic was among the first to respond to the accreditation programmes for registry service providers (RSPs). Incidentally, ICANN no longer carries out pre-delegation testing: an operator validation programme is applied upstream. Certification of the DNS (Domain Name System) has now been formalised and that of the SRS (Shared Registry System) is under way. Its presence at the ICANN meeting also provided an opportunity for Afnic to turn the spotlight on its offering as an RSP, Afnic Registry Services (ARS). Émilie Turbat, who was in charge

of the Afnic stand, can attest to the degree of interest shown by participants in the association. Apart from this, ICANN also played a decisive role in resolving the major crisis of governance that shook the African Network Information Centre (AfriNIC) when a private Chinese actor tried to dominate it. In particular it contributed to the organisation of transparent elections allowing a new Board of Directors to be appointed. The legitimacy of AfriNIC's governance was thus restored and Africa can once again be allocated IP addresses. The hefty fees applied by ICANN to geoTLDs gave rise to numerous complaints, some of them bitter, from local authorities obliged to pay them in order to be certified as such. However, the CEO would be able to adjust the price between the date of the meeting and the end of December.

Sébastien Bachollet reported that the reviews, a major subject of the evolution of governance at ICANN, were also being discussed.

Pierre Bonis then indicated that NDDCamp had been held the previous week in Brittany, at the same time as Cyber Week. Afnic, which took an active part in the event, had reminded participants of a number of matters linked to security requirements. Afnic had also taken the opportunity of turning the spotlight on the training offered by the association on securing emails.

The European ccTLDs had expressed to CENTR, Brussels, their wish to resume dialogue with the registrars. This concern was all the more significant in that the NIS 2 directive may well lead to tensions between registrars and registries. Specifically, the directive does not clearly distinguish the respective responsibilities as regards holders' data. Above all it would be important to avoid the double pitfall in which the registrars, considering themselves solely responsible, do not send any data, while the registries disclaim all responsibility. In CENTR, the TLD ISAC (Information Sharing and Analysis Centre) is an open group that brings together major European domain name actors around cyber threats.

Afnic's Scientific Council Open Day had been devoted to post-quantum cryptography (PQC), a particularly operational subject for the association. The discussions had highlighted the urgent need to roll out quantum computer resistant encryption algorithms to face attacks of the "store now, decrypt later" type. These algorithms exist, but they often require very significant calculation times. This raises the question of how to integrate them without detracting from performance, bearing in mind that security would be degraded if they were not used. Afnic and its counterparts are working to define the best trade-offs.

The latest edition of the French Internet Governance Forum (IGF) was also very successful and interesting. What is special about this forum is that it deals not just with the governance of the Internet but also more generally with subjects affecting society such as the use of AI. This is probably the Internet event that draws the highest number of students, an essential point in ensuring continuity in the field of Internet governance.

Pierre Bonis announced that, since both Sébastien Almiron and Paul Perpere would be obliged to retire by rotation in 2026, Afnic would hold elections in the registrars' and users' colleges. The outgoing trustees could be re-appointed. Since the next meetings of the consultative committees were scheduled for May, after the validation of the candidacies, the candidates would be able to express their priorities in these meetings and thus make valuable contributions to the discussions. The Board of Trustees would launch the electoral process in February.

Lastly, Afnic took part in the preparation of a special edition of the children's magazine *Astrapi* devoted to cybersecurity. On a similar line, the CNIL (French Data Protection Agency) designed manga comic books aimed at raising young people's awareness of personal data protection and privacy online.

A member wished to thank the Afnic staff for their contribution to NDDCamp, an event at which much was learnt. Some subjects were worth spreading and being discussed in the consultative committee meetings. For example, he had discovered that it was possible to make abusive use of a domain name without actually having a domain name.

Pierre Bonis reminded those present that the organisers had sent a link to the video of the event.

4. Information update and discussion items

4.1. Registrars' adoption of APIs

4.1.1. Context

Linda Caplain stated that, as part of the overhaul of its registry system, Afnic had made a third interface available to the registrars for the registration and management of domain names, in addition to the EPP and the Extranet. These standardised APIs (Application Programming Interfaces), coming as a complement to the two other interfaces, facilitated the integration and automation of operations. The .fr and the French Overseas TLDs had switched to the new solution on 1 October 2022.

4.1.2. What exactly is an API?

An API:

- allows two applications or software programs to exchange data with each other;
- serves as an interface for using the functionalities of a software program or an application;
- can be public (open to all) or private (reserved to certain applications);
- is based on REST standards, with which most web developers are familiar;

- is accessible with all programming languages.

4.1.3. Some figures by way of illustration

According to Afnic's observations, 41 registrars made regular use of APIs for .fr operations. These are small registrars; the large registrars use EPP. On average, Afnic receives 1,310,000 commands per months from APIs.

Breakdown of registrars by stock

- Large (> 100,000 Domain Names) : 5%
- Medium (1,000 – 100,000 DN) : 32%
- Small (- 1,000 DN) : 63%

Average number of commands per registrar/month

- Large (> 100,000 Domain Names) :: 9,474
- Medium (1,000 – 100,000 DN) 514,237
- Small (- 1,000 DN) :: 785,429

- **Average number of commands per registrar/month as a percentage**

- Large (> 100,000 Domain Names) : 1%
- Medium (1,000 – 100,000 DN) 39%
- Small (- 1,000 DN) : 60%

4.1.4. Practices observed

For this analysis, it was decided to divide operations into two broad categories: "read/write" and "read-only":

- a command to create a domain name (domain:create) is considered a "read/write" operation;

- a command to check the availability of a domain name (domain:check) on the other hand is considered a read-only operation

READ/WRITE OPERATIONS PER MONTH:

Small registrars < 1,000 domain names	**1,880**	**30%**
Medium registrars 1,000-100,000 domain names	**4,270**	**68%**
Large registrars > 100,000 domain names	**105**	**2%**

Read-only OPERATIONS PER MONTH:

Small registrars < 1,000 domain names	**783,550**	**60%**
Medium registrars 1,000-100,000 domain names	**510,347**	**39%**
Large registrars > 100,000 domain names	**9,369**	**1%**

The top 5 operations based on portfolio size are broken down as follows:

1. DOMAIN_INFO (461,141)
2. CONTACT_INFO (198,951)
3. DOMAIN_CHECK (70,585)
4. DOMAIN_LIST (39,382)
5. HOST_INFO (10,949)

The top 3 operations registrar's stock > 100,000 DNs

1. REGISTRAR_INFO_AUTHORIZATION_CODE_REQUEST
2. DOMAIN_CHECK
3. REGISTRAR_CREATE_AUTHORIZATION_CODE_REQUEST

The top 5 operations registrar's stock [1,000-100,000] DNs

1. CONTACT_INFO
2. DOMAIN_CHECK
3. DOMAIN_INFO
4. DOMAIN_LIST
5. REGISTRAR_LIST_REGISTRY_LOCK_DOMAIN

AFNIC'S USE OF APIS

In Afnic, the Whois directory available on the association's website uses an API to find out whether or not a domain name is subject to prior review before declaring it available and/or publishing the relevant data. APIs are also used in the context of status management during dispute resolution procedures. Many tests are also performed via APIs in order to automate them (for example, regression testing). In short, "registry" APIs are used to implement a large number of measures to check the data in the base

4.1.5. For further information

Linda Caplain gave the references of several useful resources to learn more about the subject:

- Several articles by Stéphane Bortzmeyer are available:
  - https://www.afnic.fr/en/observatory-and-resources/expert-papers/the-fr-api-for-registrars-1-4/
  - https://gitlab.rd.nic.fr/afnic/code-samples/-/tree/main/API
- Online documentation: https://api.nic.fr/api-docs/
- A script for updating contacts (eligibility and reachability) is available on simple request from the account managers.
- The same APIs are available for all TLDs operated by Afnic (.re, .pm, .paris, .alsace, etc.).

A member of the registrars' college asked whether the registrars used the APIs and whether their being made available had led to a wave of new requests for accreditation.

Linda Caplain indicated that the medium-sized clients who had been using EPP had all switched to the APIs. Other, smaller clients that had been using only the Extranet had also adopted the APIs *en masse*, particularly for interfacing verification of domain name availability. At present, there was nothing to indicate that the APIs had led to new applications for accreditation.

Émilie Turbat reported the case of a person who was absolutely delighted at the process of accreditation via API. At the ICANN meeting, discussions centred mainly on shortening the decision-making cycle for accreditation.

Régis Massé informed the meeting that the IETF was working on standardising the use of APIs in registry systems.

Linda Caplain pointed out that commands by API currently outnumbered those by Extranet.

Pierre Bonis emphasised that APIs constituted an affordable automation and simplification system. As a reminder, the major registrars had found it difficult to automate the authorisation code. It is worth pointing out that Afnic implemented APIs before the IETF turned its attention to the matter. Thanks to APIs, services such as those relating to dispute resolution can be rolled out faster than before.

Régis Massé explained that APIs also allow access to databases to be secured.

4.2. Afnic's proposals in response to State RFPs for the concession of management of the French overseas TLDs and information on changes to the Naming Policy

4.2.1. Context

Pierre Bonis stated that the Directorate General for Enterprise (DGE) had issued two RFPs for the concession of the public service of registry for ten French overseas territories. These concessions were for five years, with the possibility of extension. French Polynesia and New Caledonia were not concerned.

4.2.2. 1st RFP

Afnic had responded in July to this RFP published in June. The TLDs concerned were those of Martinique, Guadeloupe, French Guiana and the French Southern and Antarctic Lands. To date, the association had received no response or invitation.

4.2.3. 2nd RFP

Initially announced for 2026, this RFP was published on 28 October 2025. The deadline of 28 November was set for the submission of offers. The TLDs concerned are those of Mayotte, Wallis and Futuna and Saint Pierre and Miquelon. A proposal would be made to the Board of Trustees not to respond in respect of .mf (Saint Martin) or .bl (Saint Barthélemy). Firstly, these TLDs were not delegated in the DNS root zone. Secondly, in application of the Post and Electronic Communications Code, only TLDs reserved for the national territory can be tendered for, and this is not the case. Lastly, the representatives of these territories' local authorities had not specifically expressed the wish to activate these TLDs.

4.2.4. Response to the RFPs

Afnic had submitted an application which included all its commitments for management of the .fr TLD, with the exception of the financial commitments to fine-tune rates (for the .fr TLD, these commitments correspond to a percentage of turnover, which would not be an appropriate criterion for the overseas TLDs in view of the turnover expected). The bulk of the commitments relate to technical, SLA and security aspects (all ccTLD registries being essential entities). The registry policies applicable to the .fr TLD (dispute management, dealing with abuse and pricing policy) would apply equally to these TLDs. Lastly, local consultation and agreement was envisaged around the overseas question, and the major awareness-raising programmes on the digital transformation would be rolled out in these territories.

Pierre Bonis added that Afnic would encourage the creation of two or three local registrars (a streamlined accreditation formula was planned). Apart from this, the next Anycast node would be deployed in the Caribbean to improve the DNS resolution service. There were also plans for a one- and two-character opening phase for the TLDs won by Afnic, which would be a source of additional revenue.

4.2.5. Information on changes to the Naming Policy

Depending on the TLDs awarded to Afnic by the State, the following are envisaged:

- consultation and agreement with members and also with the territories concerned;
- a public consultation on the proposed amendments to the Naming Policy;
- validation by the Board of Trustees of the amendments to the Naming Policy.

For TLDs not already under Afnic's management, negotiations will be required with the outgoing manager and with IANA, the Internet Assigned Numbers Authority. Afnic members will be asked to show that the change of management is in line with the interests and expectations of the Internet community.

A member wished to know whether the opening to one- and two-character names would affect holders of prior rights or whether there would be a landrush.

Marianne Georgelin indicated that there were plans to organise a public consultation on how to open registration.

Pierre Bonis explained that the aim with this kind of operation was to protect the rights of rights holders and not to allow added value to be appropriated by intermediaries. This added value should accrue to the registry, for financing the actions directed at the territories concerned.

4.3. NIS 2: update on the transposition of Article 28

4.3.1. Progress so far

Afnic is still awaiting the transposition into French law of the NIS 2 directive (France is one of the eight countries that have not yet transposed it). Incidentally, Pierre Bonis lamented the fact that the majority of EU Member States were apparently incapable of sticking to the time frame that they themselves had approved for this transposition. The senate committee's review (*https://www.senat.fr/tableau-historique/pjl24-033.html*) had now been completed. The review by the plenary session of the National Assembly was scheduled for January 2026, after which the bill would go back to the Senate for a second reading before returning to a plenary session of the Assembly or a *Commission Mixte Paritaire* (CMP, a joint committee to resolve disagreements between the two chambers). ANSSI, the National Cybersecurity Agency, recently opened its pre-registration platform for entities that expect to be required to register under the NIS 2 directive when it is transposed (*https://club.ssi.gouv.fr/#/nis2/introduction*).

A member of the College of Registrars pointed out that ANSSI's website offers a tool whereby an entity can find out whether it is concerned by the directive.

Pierre Bonis stressed that Afnic's understanding was still that open registries are essential entities and that the registrars are concerned by the NIS 2 directive by virtue of Article 28 on the verification and quality of information for identifying and contacting the holders (Article 19 in the transposition). However, whether or not an entity was essential depended on the service offered, not on this Article. Most registrars were considered essential entities since they hosted domain names on authoritative servers for the zone (not only top level). The obligations imposed on essential entities were mainly those involving the organisation of cybersecurity. Specifically, the NIS 2 directive requires an information security management

system to be put in place as part of a continuous improvement approach to cybersecurity based on risk analysis. This analysis will naturally vary depending on the size of the registrar. Consequently, the resources deployed will be in proportion to their activity, a position currently shared by ANSSI. Afnic will support the registrars by means of various mechanisms at the association's disposal and the training courses that it makes available (the "Lead Implementer" course, designed mainly for CISOs, and a less intensive course on cybersecurity which should be enough initially for small registrars.)

4.3.2. Afnic's actions:

In committee hearings, we were able to have the words requiring holders' identity to be verified "upon collection" eliminated. We stressed that this looked like *ex ante* verification, which could give rise to problematic interpretations. Meanwhile other amendments were proposed by collective management organisations. One of them recommended that the data verification procedures be set forth in a decree. The directive requires the instructions to be transparent, published and accessible. In principle, Pierre Bonis remarked that this amendment constituted a big step backwards for the multi-stakeholder system that exists for the .fr TLD. Registry policy verification procedures were indeed subjected to public consultation and approved by the Board of Trustees. Since the birth of the .fr TLD, the registration rules have never been drawn up in an office of the Ministry of Economics and Finance. In practice, the verification systems evolve as improvements become available. If the rules were defined by decree, they would remain fixed. These arguments were defended in talks with the DGE and ANSSI, and the State had issued an unfavourable opinion on these proposed amendments.

Marianne Georgelin pointed out that Article 28 concerns the registrars. The risk was therefore that verification procedures would be imposed on them by decree. So it is important to be very vigilant on this point.

Pierre Bonis added that collective management organisations had proxies in their sights, wrongly considering them as agents of the registrars, and were demanding that anonymity be lifted. Be that as it may, ANSSI and the DGE shared Afnic's positions.

A member was afraid that he might be subject to the NIS 2 directive by virtue of the domain names he managed for his relatives.

Pierre Bonis explained that consideration as an essential entity applied only to the hosting of domain names for third parties.

Another member assumed he would be considered an essential entity in that he managed the domain names of his associations.

Pierre Bonis put forward the view that the relationship was not a commercial one. It must also be borne in mind that the sanctions linked to NIS 2 would be decreed by a committee called by the Director General of ANSSI, not by a judge. The priorities that ANSSI had expressed as regards proportionality should enable absurd situations to be avoided.

In reply to a question, Pierre Bonis cited some examples of collective management organisations: ADAMI, SACEM, SACD, etc. In parliamentary debates, they were generally represented by the SDPC. Afnic countered their strategy of seeking to influence the legislator with a bottom-up, multi-stakeholder approach.

4.4. Study of the V2 renewal rate

4.4.1. Definitions

Loïc Damilaville indicated that the retention rate measured the proportion of names in stock that were already present in the stock 12 months before and have not been

deleted or recreated in the meantime. It differed from the renewal rate, which seeks to measure the proportion of names "extended" among those expiring during a given period. The difference between the two rates increased with the proportion of "multi-year" names in the stock. The retention rate was that used for benchmarking with other ccTLDs or gTLDs.

4.4.2. Context

Since 2022, the retention rate of the .fr TLD has deteriorated, as have those of other European ccTLDs. In order to gain a better understanding of the factors at play, an initial study was conducted in 2024; the 2025 study is a more in-depth investigation of this initial study.

4.4.3. Overview

There is a strong negative correlation between the retention rate and the creation rate. With some exceptions, the TLDs with very high creation rates have low retention rates, and vice-versa. With a creation rate of between 82% and 83% and a retention rate of between 19% and 20%, the .fr TLD is within the normal matrix.

Ret. rate / Cr. rate	15 % and less	16-25 %	26-35 %	36-50 %	51 % and more	Total	%	% 2023
86 % or more	68	10	6	2	3	89	16 %	*17 %*
76 % à 85 %	37	86	32	7	5	167	31 %	*29 %*
66 % à 75 %	3	52	64	23	9	151	28 %	*33 %*
51 % à 65 %	1	5	16	27	18	67	12 %	*13 %*
50 % et moins	1	6	4	9	46	66	12 %	*9 %*
TOTAL	110	159	122	68	81	540		
%	20 %	29 %	23 %	13 %	15 %			
% 2023	*21 %*	*27 %*	*24 %*	*12 %*	*16 %*			

Breakdown of nTLDs by Creation rate and Retention rate in 2024

Source: Afnic 2024 Global Domain Name Market Observatory report

Ret. rate / Cr. rate	15 % and less	16-25 %	26-35 %	36-50 %	51 % and more	Total	%
86 % or more	18	3	-	-	-	21	50 %
76 % à 85 %	3	11	1	-	-	15	36 %
66 % à 75 %	-	1	5	-	-	6	14 %
51 % à 65 %	-	-	-	-	-	-	-
50 % et moins	-	-	-	-	-	-	-
TOTAL	21	15	6	-	-	42	
%	50 %	36 %	14 %	-	-		

Breakdown of a sample of ccTLDs by Creation rate and Retention rate in 2024

A new KPI was introduced this year, namely volatility. This indicator associates the creation and retention rates.

So, for example, the increase in volatility of the .fr TLD observed in 2024 came in part from the increase in create operations, but in much greater part from the increase in delete operations (deteriorating retention rate). This volatility rate provides a benchmark and also gives some idea of the dynamics underlying a TLD. Lastly, for forecasting, it enables us to use “triangulation” to reinforce assumptions regarding creation and retention rates.

4.4.4. Age of names

The 2024 study turned the spotlight on the strong correlation between the age of names and the probability of their being retained. In 2025 we compared the situation at 31/12/21 with that of 31/12/24. This comparison shows that, although the rule holds true, retention rates, even for the oldest names, are affected by an erosion phenomenon.

For example, 90% of names ten years old and more were renewed in 2024 as against 95% in 2021. Similarly, the 90% threshold was reached after five years in 2021, as against seven or eight years in 2024. There may be many reasons for this phenomenon, and they remain to be investigated. A further indication is the fall in the retention rate in the first year, which dipped below 68% in 2023-2024.

Benchmarking also throws light on an additional explanatory factor by highlighting the creations/retentions dynamic. The. fr TLD is one of the most dynamic as regards the creation rate; it is "logically" less well placed in terms of retention rate.

The "oldest" TLDs, in other words those that grew faster and had a higher proportion of old names than .fr, such as .de and .nl, have higher retention rates, but also lower creation rates.

4.4.5. "Quality", a factor being explored

The quality of a domain name from the point of view of a registry or registrar could be evaluated through the manner in which it is used. It is only indirectly linked to the value of the name that is so beloved of domainers. But connections are possible: a much-used name has greater value than an unused one, since it generates spontaneous traffic, and has a better "rating" for indexing, etc.

In 2025, we studied the .fr portfolio and established the proportions:

- of names that were inactive from the web point of view (http ko);
- of names that were active from the web point of view (http ok) and of redirected names among them;
- by deduction, of names pointing to web contents, regardless of their nature;
- of names that were active or inactive from the email point of view (MX ok or ko);
- of names that were MX ok and http ok;

- of names that were MX ok and pointing to web contents, regardless of their nature.

The study of retention rates by type of use shows that 38.1% of http_ko names were deleted after the first year (as against 34% for the names covered), and that this percentage fell in the following years, to an average of 20%.

Names pointing to content regardless of their nature held steady at 65.4% in the first year, subsequently rising to nearly 85%. Redirected names were clearly better retained (89.4%), but showed little improvement thereafter (91.8% on average). Overall, names associated with emails show higher retention rates than those associated with web browsing.

The surprising factor is the relatively low retention rate of "content" (65.4% in the first year, then 84.9% on average) and of "emails and content" (67.7% in the first year, then 85.6% on average). We would need to investigate the content to understand more and, for example, to be able to isolate genuine websites from holding pages and parking pages with sponsored links. It is more than likely that the low overall score conceals some very different dynamics depending on the nature of the content.

The breakdown of .fr names by type of use associated with historical retention rates will in due course allow probability assessments of retention rates to be produced for a given portfolio profile.

The following matrix illustrates level 1 of the predictive framework, but could subsequently be enriched with other factors identified, such as the age of names, the nature of the holders, the business model of the registrars concerned, etc.

Type of use	Vol. Stock	% Portfolio	Historical retent. rates	Retention volume
WEB BROWSING				
http_ok				
http_ko				
Redirections (of http_ok)				
Content				
Included real websites				
Included parking page / sponsored links				
Included waiting pages and others				
TOTAL .FR				
Probability assessments of retention rates				
USE OF EMAIL				
Email				
Email and http_ok				
Email and content				
Included real websites				
Included parking page / sponsored links				
Included waiting pages and others				
TOTAL .FR				
Probability assessments of retention rates				

Another management KPI, the survival rate, is calculated as the volume of a category of names at a given moment of year N as a proportion of the stock of the same category at 1 January (at 31 December, it is equal to the retention rate). This indicator allows deviations from historical averages to be identified.

4.4.6. Summary

Loïc Damilaville indicated that two predictive frameworks were used:

- the portfolio structure by age of domain names, associated with average historical retention rates for each age band;
- the three-factor framework consisting of the creation, retention and volatility rates allowing coherent assumptions to be made by triangulating the three factors.

There are also two additional management tools:

- The analysis of the seasonality of creations and deletions;
- the survival rate.

4.4.7. Lessons learned

The 2025 study served to confirm the lessons of 2024 while at the same time extending them and exploring other paths. The primary key factors remain the general dynamics of the TLD with the three-way interplay between volatility, creation and retention, the age of names and the nature of holders. There are also other analysis factors, namely the registrars' business model and the types of use. Two KPIs have also been integrated with the dashboard - the volatility and survival rates.

4.4.8. Lines of action

Loïc Damilaville listed several lines of action:

- continue to explore content types in order to obtain a third predictive framework;
- test the accumulated knowledge by preparing an integrated predictive model that can be used for 2027;
- work with the registrars and with Afnic's counterparts in CENTR on other parameters that may affect retention rates (CENTR has a much more mathematical approach, which could be complementary);
- continue to raise registrars' awareness of the importance of the retention rate;
- urge those registrars that have not yet done so to implement billing procedures that encourage renewals in the three years following creation;
- evaluate the weight of the blocks of multi-year names that started appearing at the end of 2024 so as to be able to anticipate their expiry and integrate this phenomenon into the forecasts from 2027 on.

Loïc Damilaville stressed that the proliferation of multi-year offers by certain major registrars could become a significant factor of uncertainty, altering the maturity structure of the .fr portfolio. Some new names will be retained in 2025 and 2026 without having had to be renewed, and not maturing until 2027.

Pierre Bonis explained that the exercise conducted consisted in understanding the dynamics and anticipating them. The question now is whether the registrars see ways to improve the retention rate.

A member of the users' college remarked that mathematical models described the past but were predictive only in an extremely stable universe with no interactions. The studies conducted by Loïc Damilaville, being based on qualitative elements observed, had a strongly predictive dimension.

Loïc Damilaville explained that CENTR paid close attention to the time for which holders had held domain names. Thus he observed that the longer a holder had been a holder, the more likely they were to have a quality domain name. The time series analysed would admittedly highlight some phenomena that will be explained by qualitative data such as ease of registration.

Pierre Bonis observed that if time as a holder was an explanatory factor, this reduced the ability to increase the renewal rate — it is not possible to achieve ten years as a holder in just one year. It was necessary to rely on a large number of small actions, which would contribute to creating domain names that would gradually age, but this would not lead to rapid recovery.

A member of the users' college said he thought the registrars should focus more on multi-year offers. As regards practices, messaging is still too complicated for users. Yet messaging is precisely one of the main uses of a domain name for users. Next year will mark twenty years since natural persons were first offered the possibility of buying a domain name. We should seize the opportunity and envisage actions in favour of individual users.

Pierre Bonis reported that during September's strategic seminar the question of communication to the general public was addressed, and that this relates directly to the public uses of domain names. Apart from this, the registrars' proportion of

multi-year agreements was growing strongly, reaching 14% and placing Afnic well above its counterparts.

The same member also spoke in favour of more targeted actions. The personal addresses of certain professionals (MPs, captains of industry, etc.) are sometimes staggering. It would be good for a page of Afnic's website to present the advantages of having one's own domain name.

A user member asked whether a correlation had been established between commercial operations and the slippage in the first year retention rate seen in 2023. He also observed a significant concentration of a small number of registrars in France, which could make the .fr TLD an exception in Europe.

Émilie Turbat indicated that the commercial operations performed better than the .fr TLD as a whole as regards renewals. These operations were custom designed with the registrars and were intended to support launches. As regards the concentration of registrars, the other European countries experienced the same phenomenon.

Pierre Bonis endorsed this and added that every country had a "top ten" concentrating 90% of registrations.

Émilie Turbat added that Afnic was the only ccTLD operator to carry out customised commercial operations. The others tended to resort to the "one size fits all" technique and to discount campaigns.

Éric Lantonnet reported that OVH had launched a three-year registration operation on its website on an experimental basis.

A member of the college of registrars indicated that this operation had been a success and that it had been renewed, although the objective had been attained

faster than had been foreseen. The promotional multi-year offer is shown as being for three years by default.

Pierre Bonis insisted on the fact that such operations were beneficial for both Afnic and the registrars. In passing, the latest projections show that the 2% of turnover rebated to the registrars for commercial operations will be exceeded in 2025.

4.5. Points raised by members

One point was raised by the registrars, none by the users.

QUESTION ON AFNIC'S DEALING WITH ABUSE:

In practice, it can occur that:

- a registrar's client account is compromised and the associated means of payment used fraudulently;
- or an account created with stolen means of payment is used to register domain names.

In these situations, the registrar usually deletes the domain names concerned. In addition to the charge-back expenses levied by the payment service provider, the registrar also has to bear the cost of the fraudulent registrations.

It might make sense to establish a specific reimbursement procedure for such cases. Such a procedure should naturally have built-in safeguards: the registrar would have to show that the fraud has actually taken place and, if possible, present the measures taken to avoid this happening again.

The current situation now leads to Afnic's benefiting directly from fraudulent registrations, which seems questionable.

Pierre Bonis expressed his disagreement with this last point. These registrations had effectively been created and it was therefore normal for Afnic to be remunerated accordingly. Furthermore, a mechanism exists – the grace period – allowing the registrar to avoid this kind of situation. Registrars that use it soon realise that the means of payment used had been stolen. If Afnic were to reimburse registrars for fraudulent registrations beyond this period, the distribution network would have no incentive to invest in verification. The grace period constitutes a form of room for error: if the domain name is deleted soon enough, it is not invoiced. In the past, Afnic had managed to deal with some very specific cases, but by taking a commercial approach.

A registrar member pointed out that this rule was applied by many top rank registries, including Verisign. The registrars check the email addresses and telephone numbers, but for means of payment they are reliant on their payment service providers. They do not find out about a fraudulent payment until the owner of the means of payment discovers it. What is more, the payment service providers bill the registrars, since they have to reimburse the owner. Hence the above request from the registrars.

Pierre Bonis said he understood that the rule was not satisfactory but, again, the registrars could obtain reimbursement providing they requested the deletion of a domain name before the end of the grace period.

Éric Lantonnet said it would be interesting to know how many registrars were concerned and the amounts involved. He had personally had to approach Afnic regarding the erroneous renewal of hundreds of .fr domain names. In view of the particular circumstances, Afnic had granted a special gesture of goodwill.

One of the members of the Users' College wanted to know whether Afnic had the right to check the means of payment required by the registrars.

Pierre Bonis replied that it did not.

A registrar member said it was the registrar's responsibility to specify what means of payment it accepted. The registrar that he represented had a scoring system which allowed persons or entities identified as fraudulent to be excluded.

Another registrar member also explained that the banks offer insurance. It is not up to Afnic to cover the cost of insurance that had not been taken out in order to save money.

The registrar member conceded that these frauds were not an everyday occurrence. They generally arose periodically. The registrar that he represented also used a scoring tool. Fraudsters have access to millions of stolen means of payment, and their registrations are not always easy to identify. They use money-mules, who go from one registry to another, with different TLDs and accounts. Losses can be as much as €100,000.

Pierre Bonis undertook to hold discussions with the registries, if any, that agreed to reimbursement beyond the grace period providing the registrar could prove that the means of payment used were fraudulent. In any case, this practice would constitute a profound change in Afnic's registry policy. Specifically, it would be tantamount to confirming that a significant number of domain names had been registered by way of identity theft and that Afnic had consequently developed a procedure for reimbursing the wronged registrars. Such a signal would not be well received in the context of the transposition of the NIS 2 directive as it relates to verification of a holder's identity.

A member informed the meeting that the .dk and .se TLD registries already applied the proposed rule. Beyond the monetary aspect, it would be good for Afnic to be informed by the registrars of the domain names concerned so as to be able to inform the other registrars in turn.

Marianne Georgelin explained that alerting the registrars would be difficult if we relied solely on domain names, since in cases of fraud the holders changed constantly. She also considered that it would be interesting to know the amounts involved.

A registrar member suggested establishing a redemption period between the deletion of a domain name as a result of a fraud and the possibility of re-registration, thus alerting the remaining registrars and enabling them to carry out additional checks.

Pierre Bonis indicated that this raised the question as to whether Afnic should consider a domain name deleted by a registrar due to fraud as a domain name that it would have deleted itself due to abuse. In such case, the domain name would be subjected to in-depth verification.

5. Subjects submitted for consultation

5.1. Implementation of two-factor authentication (2FA) for connections to Afnic's extranets

Marianne Georgelin announced that implementation of two-factor authentication (2FA) for registrars to log on to their .fr and French overseas TLD accounts was to be made mandatory. Implementation of two-factor authentication was currently a basic good cybersecurity practice according to ANSSI and the CNIL in particular.

Certain recent incidents affecting registrars and involving data theft lend weight to the well-foundedness of this good practice and remind us that the threat of theft of log-in data is all too present, specifically in the domain name management business.

By reducing the risk of illicit log-ins to Afnic's extranets with registrar accounts, the registrars' activation of 2FA is a win-win situation:

- For holders: it protects them against harm linked to undesired alteration of data associated with their domain names (deletion, change of name servers, etc.) that may arise if an attacker managed to log on to one of Afnic's extranets by making fraudulent use of a registrar's compromised credentials.
- For the registrar: it reduces the likelihood of a registrar's having to manage an incident resulting from the ill-intentioned use of one of its accounts on an Afnic extranet.

This type of incident could lead to:

- an obligation to notify the CNIL (Data Protection Agency) and possibly the holders (data subjects) in the registrar's portfolio, of a personal data breach;
- possible sanctions imposed by the CNIL for non-compliance with Article 32 of the GDPR.

Although all the extranets (.fr, the French overseas TLDs and the gTLDs) already offer each user of a registrar account holder the possibility of activating two-factor authentication, the rate of uptake of this measure remains low relative to the extra security it provides.

TLD	Active accounts	Pourcentage 2FA activated (20/09/2025)
FR	1,085	23 %
PM	796	9 %
RE	801	11 %
TF	790	9 %
WF	789	10 %
YT	791	10 %

With effect from 7 April 2026, activation of two-factor authentication will be indispensable for accessing the .fr and French overseas extranets. This marks an important step forward in the protection of accounts and the security of information exchange. Registrars are encouraged not to wait for this deadline but to activate this simple, quick security measure now so as to ensure the continuity of their secure access.

Pierre Bonis stressed that making two-factor authentication mandatory stemmed from the proven materialisation of the risk of compromised credentials. In parallel with this, Afnic is jointly responsible for the processing of holders' personal data. Since the CNIL sees 2FA as a good practice, a registrar not activating it despite its being made available by Afnic would find itself in a difficult legal situation if its account were to be compromised.

A User member stressed that 2FA worked poorly, especially when the code was sent by email, with waits often exceeding five minutes.

Another member pointed out that 2FA was used by most registries. Besides, there are several types of 2FA. The type that works by email is not the best. The TOTP (Time-based One-Time Password) is far more effective.

Nicolas Pawlak added that the advantage of the TOTP was that the technology was available offline. Even if it is not connected to any network, a telephone can still generate a code without going through SMS or email.

A member asked whether 2FA applied to interactive use or to the APIs.

Régis Massé specified that 2FA would be applied to the extranets. The APIs would be reinforced by means of certificates. The 2FA used would work with TOTPs. When first logging on with 2FA, registrars would be asked to scan a QR code to obtain a six-figure code to be input. A reset procedure in case of loss or theft of the telephone was in the final stages of preparation.

5.1.1. Feedback from the Registrars' and Users' Committees

5.1.1.a. Users

The Users' Committee approved the move to secure exchanges between registrar and registry, since it favours users and security. Some points however still need to be clarified, among them the protective measures put in place (could a restriction of the registrar's IP addresses be envisaged?). The committee sought a happy medium between security and practicality Indeed, having to input a TOTP code on each log-in could be problematic. Extending the validity to a day or a week would remedy this. The committee also mentioned the possibility of an SSO or MFA type solution. It was surprised by the current low rate of uptake.

5.1.1.b. Registrars

The Registrars' Committee approved the principle of 2FA for accessing Afnic's interface and the calendar envisaged for its implementation. It had questions however regarding the procedure for deactivating it in the event of loss or impossibility of access. Also, the possibility of white-listing IP addresses could be envisaged.

Afnic responded in part to the committees' questions and observations and indicated that it would examine the rest later.

As regards white-listing IP addresses, Régis Massé explained that a registrar may need to log on from abroad in order to work, in which case its IP address cannot be blocked. This was the reason the 2FA route had been decided on. The possibility of white-listing could however be studied.

Pierre Bonis reaffirmed that if a majority of registrars campaigned for white-listing of IP addresses, the measure would be put in place. It should however be borne in mind that this way of working would be somewhat rigid in practice.

Régis Massé recalled that an SSO was an authentication system allowing a user to log on to several applications or websites with a single password chosen upon his or her first log-on. It could not be used within Afnic, because the registration system was partitioned among the various TLDs. Furthermore, the NIS 2 directive required the various environments to be isolated from one another. TOTP tokens should be valid for at least an hour (subject to verification).

Pierre Bonis pointed out that use of the web services was very much *ad hoc*. A one-hour duration was therefore appropriate.

5.2. Improvement of technical and operational documentation and operational communication

Élodie Belliard presented the results of a survey of registrars conducted between December 2024 and February 2025 on technical and operational documentation and operational communication. Of the 37 respondents, 26 answered the entire survey.

By way of reminder, technical documentation comprises:

- the Technical Integration Guide;
- the API REST Guide.

Operational documentation:

- the Procedures Guide;
- the functional documentation of the .fr TLD.

Operational communication:

- Communication on maintenance;
- the sending of release notes.

The main results of the survey are as follows:

Ease of access to documentation

TECHNICAL INTEGRATION GUIDE

- 33% of respondents considered that all the necessary information was provided;
- 26% would like additional examples of EPP commands;
- 26% need specifications/clarifications on operations described in the Guide;
- 11% would appreciate detailed explanations of common errors.

Satisfaction and quality of operational documentation

FUNCTIONAL DOCUMENTATION OF THE .FR TLD

- 57% of respondents considered that all the necessary information was provided;
- 22% would like specifications or clarifications on operations described in the Guide;
- 17% would appreciate detailed explanations of common errors.

PROCEDURES GUIDE

- 65% of respondents considered that all the necessary information was provided;

- 13% would like specifications or clarifications on operations described in the Guide;
- 9% would appreciate detailed explanations of common errors.

Operational communication and release notes

OPERATIONAL COMMUNICATION

- 88% of respondents find operational communications regarding maintenance dates and affected services sufficiently clear.

RELEASE NOTES

- 100% of respondents were satisfied with the frequency of dispatch of release notes.

- • 78% of respondents prefer to receive release note notifications as email attachments, 19% prefer to view them via their Extranet account in the News section (and 3% prefer Other).

Élodie Belliard indicated that, with the help of these results, it had been possible to define four strategic action paths:

- optimise technical and functional documentation: Time saved, improved understanding and autonomy;

- schedule communications via preferred channels: Visibility, clarity and error reduction;

- “live” documentation and shared updates: Trust and transparency;

- rethink access to information: Make searching and consultation easy and accessible.

Élodie Belliard then listed the proposals made:

1. Centralise documentation

- a single shared space;
- clear tree diagrams;
- a search functionality;
- tracking of documentation versions;
- integration of release notes and history.

2. Content and updating of documentation

- review documentation to make it more readable when necessary;
- perform regular updates (enrichment of content and clarifications).

3. Accessibility of documentation and release notes on the extranet

- make the documentation accessible from the main menu on the left;
- tracking of documentation and release notes versions.

4. Notification channels and review of calendar

- Communication by email:
  - announcement on D-30;
  - reminders on D-15/D-7 and D-2;
  - notification of start and end of maintenance work.
- Communication on afnic.fr:
  - calendar of notifications.

- Communication on the extranet account:
    - information banner at the top of the Extranet: day D of maintenance, beginning and end and in case of extension.

5. Improved readability for registrars and holders – afnic.fr

Maintenance calendar:

- highlight upcoming maintenance dates;
- use colour coding to distinguish the various kinds of maintenance;
- information via hover;
- link to detailed operational communication.

New organisation:

- separate future maintenance operations and those under way from completed ones;
- automatically arrange in chronological order;
- filter by environment, TLD and month/year.

6. Maintenance operations visible on the extranet account

Maintenance calendar:

- highlight upcoming maintenance dates;
- use colour coding to distinguish the various kinds of maintenance;
- information via hover;
- link to detailed operational communication.

Maintenance page:

- Post a maintenance page when the Extranet is inaccessible, throughout the duration of the maintenance.

Élodie Belliard noted that success indicators had been defined:

Theme	Main indicators	Method
Accessibility of documentation	Percentage of clients satisfied with the ease of access to the documentation	Satisfaction survey after application of recommendations
Clarity of documents	Average clarity score (out of 5) awarded by the registrars	Satisfaction survey after application of document revision
Updating of content	Percentage of the documents up to date 72 hours after publication Percentage of registrars that consider the documentation to be clear and up to date	In-house monitoring of the changes needing to be made
Integration of customer feedback	Percentage of feedback integrated in documentation	Satisfaction survey
Communication of upcoming maintenance operations	Percentage of clients informed at D-30 of a maintenance operation (open rate) Satisfaction rate on the quality of email announcements Satisfaction rate on the maintenance calendar	Monitoring by means of the emailing tools Satisfaction survey after application of recommendations

Pierre Bonis specified that although the survey had concerned registrars, the documentation could also be accessed by users. He also thanked the registrars who had taken the time to respond to the survey.

The discussions between the members and Afnic allowed the following points to be clarified: Régis Massé said that Afnic was working to provide more real-time information on maintenance operations, to reduce the time taken by them and to be able to continue communicating even in times of crisis.

5.2.1. Feedback from the Registrars' and Users' Committees

5.2.1.a. Users

The Users' Committee would like information on the respondents' profiles. It was unanimously agreed that making the documentation available to as many people as possible was a good thing. On the other hand, what about the work and the resources necessary to improve its content?

5.2.1.b. Registrars

The Registrars' Committee suggested adding a system of .ics files or RSS feeds. It recommended keeping in place the email announcing maintenance and adding more detail if possible. It asked to which address the email was sent. It also asked for the email to specify exactly how long the maintenance would take.

Afnic responded in part to the committees' questions and observations and indicated that it would examine the rest later.

Pierre Bonis specified that Afnic was not able to indicate in advance exactly how long a maintenance operation would take.

Élodie Belliard indicated that the questionnaires were anonymous and it was therefore not possible to know the respondents' profiles.

As regards resources, Pierre Bonis explained that the time devoted to improving the documentation would be monitored.

5.3. Detection of registration data contrary to the Naming Policy upon creation of the domain name: extension and development of the system

Marianne Georgelin presented this system, also known as FR Check, which had been implemented in September 2023 following a public consultation and which mainly concerned users.

COMBATING ABUSE: USER PROTECTION

The fight against abuse has a threefold objective:

- to retain the trust of .fr users in the national TLD;
- to quickly and effectively put an end to the abusive practices of certain holders, while respecting the rights of each individual and maintaining the necessary neutrality of the registry, both indispensable elements of this trust;
- and to develop Afnic's practices, in particular by means of innovation, so that strengthening the fight against abuse is consistent with maintaining the simplicity and competitiveness of the .fr domain, in a context of heightened competition.

The objective of the FR Check system is to identify, as soon as a domain name is created, and before it is published in the DNS, the particulars of holders who do not comply with the eligibility criteria of the .fr Naming Policy. From the outset, it was decided to apply the criterion of holder eligibility, this being the main criterion for accessibility to the . fr TLD.

This mechanism makes it possible to probe all .fr domain name create operations and to automatically identify those for which the holders have given the country code of a country outside the EU and EFTA.

Whenever a domain name for which the holder's particulars correspond to this category is detected, the domain name is registered, but not published in the DNS. This means the domain name is registered in the name of its holder, but its publication in the DNS is temporarily suspended for seven days. This being so, the services associated with the domain name, such as the website, email address, etc., are not, *de facto*, operational. The domain name had not yet been exploited.

A verification procedure is then launched at the end of the seven-day suspension period; it is applied as follows:

- automatic blocking of the portfolio of the holder of the domain name detected;
- automatic notification of the holder and the holder's registrar of the start of the procedure;
- duration of blocking: 30 days maximum.

A user member observed that if a holder had a portfolio, that holder must by definition already have registrations. He struggled to understand why, if non-eligibility was detected on the occasion of a new creation, all the other domain names should also be deleted. He quoted the case of a registration made in the UK before Brexit.

Marianne Georgelin specified that the holder's data examined were the same for all the domain names registered in a given portfolio. Registrations made in the UK prior to Brexit would not be deleted — prior legitimacy was recognised.

A member asked whether the holder was informed of the seven-day suspension.

Marianne Georgelin confirmed that an email was sent automatically to the holder and to the registrar.

Pierre Bonis pointed out that a particular feature of FR Check was that it blocked the domain name even before it was published. Strictly speaking, the first seven days did not correspond to the verification procedure. This procedure was triggered only if the holder was unable to show good faith in those seven days.

Marianne Georgelin then set out in detail how it was proposed that the system would evolve.

When the system was launched it was envisaged that, following a period of observation reserved to the automatic detection of registrations carried out by ineligible (non-EU) holders, Afnic would seek feedback from its registrars and from users of the .fr TLD, with the help of the Consultative Committees. Since this system came into force, the publication of 571 domain names had been temporarily suspended.

Afnic now proposed to expand and develop the detection criteria used by this system, the priority still being to keep the procedure for registering domain names simple, effective and undemanding, targeting only domain names with a high risk of abusive practices.

CHANGES IN THE SYSTEM CRITERIA

With effect from 5 January 2026, the detection criteria for registration data of holders that do not meet the eligibility criteria of the .fr Naming Policy will change as follows:

- the telephone number must conform to a syntactically correct format and be validated (reachable);

- the email address must be reachable (messaging servers of the domain name of the messaging address configured in the DNS).

Nicolas Pawlak asked whether a holder could register a domain name under .fr using a foreign telephone number, assuming the format conformed.

Benoit Ampeau replied yes, adding that the syntax and the consistency of the number would be checked.

On the subject of emails, Nicolas Pawlak then indicated that it was possible to have a messaging service without an MX server. He also raised the question of providers of disposable email addresses like YOPmail.

Marc Van Der Wal said account had been taken of messaging services without MX servers. If the MSI is configured (and is not a null MX) and if an A record is present, the email address is valid.

Pierre Bonis said that disposable email addresses would be accepted with an MX server.

A member asked how many portfolios were associated with the 571 domain names for which publication had been temporarily suspended.

Pierre Bonis replied that in most cases these domain names did not hide a distinct portfolio. The procedures applied to the holder, not to the domain name. If a holder has not been detected as non-compliant for a certain time, Afnic is entirely justified in getting rid of that holder's entire portfolio.

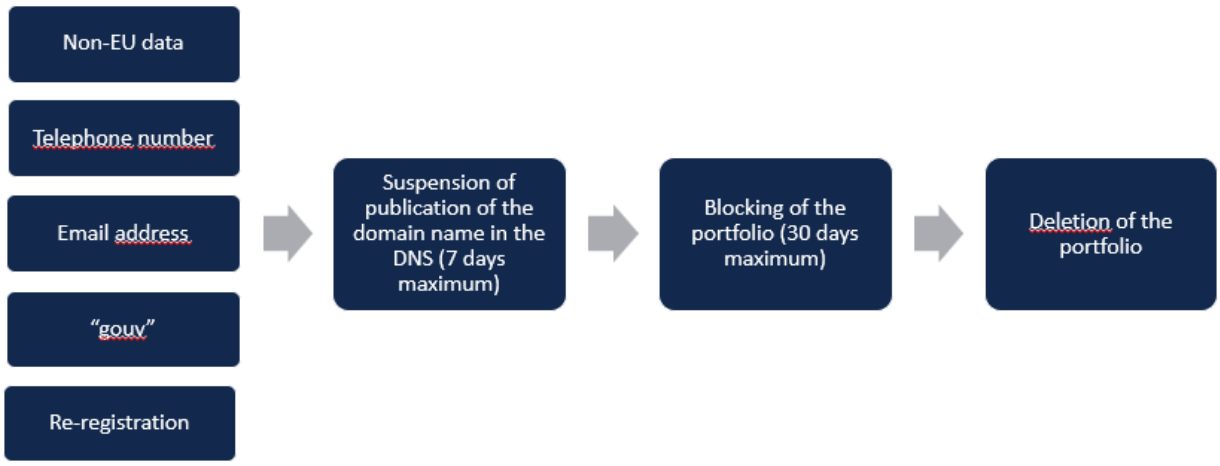
Marianne Georgelin continued by indicating that the FR Check system would be expanded to detect the use of the term "gouv" in the composition of the domain name:

- the use of the term "gouv" is reserved to the French government (see Article 2.5 of the Naming Policy);
- registration of a domain name with the term "gouv" is subject to authorisation by the SIG (Government Information Service) and it is forbidden to register domain names ending in "gouv.fr" or their IDN versions;
- verification of eligibility and reachability of the holder.

If a domain name with this term is detected, registration is suspended for seven days in which the holder must justify the data.

With effect from 5 January 2026, the FR Check system will be expanded to detect domain names re-registered in the month following their deletion due to non-eligibility or non-reachability after a verification procedure. In a three-month test period, 383 domain names were re-registered in the month following their deletion. For these names, eligibility and reachability will be checked again to make sure they have not been re-registered with the same defects as before.

With effect from 5 January, the system will operate as follows:



In the test period from 1 September to 31 October 2025:

- telephone number: 1,629 domain names detected;
- email address: 123 domain names detected;
- use of the term "gouv": 17 domain names detected (including three false positives);
- registration of a domain name subjected to a verification procedure leading to deletion less than six months before its new creation: 383 domain names detected (the test will be modified to reduce the period to one month).

Pierre Bonis pointed out that on average there were 75,000 create operations every month.

A member asked why it was proposed to reduce to one month the period for detecting domain names that have already been subjected to a verification procedure leading to deletion.

Marianne Georgelin explained that the tests had shown that nearly all re-registrations of domain names following deletion as a result of verification

procedures took place in the month following this deletion; hence the recommendation to use the one-month period.

Pierre Bonis added that the aims were to avoid scams and to avoid associating Afnic's procedures with a poor image. Ill-intentioned people did not wait six months before trying to re-register a problematic domain name.

A member of the Registrars' Committee asked why Afnic did not establish a blacklist of these domain names.

Pierre Bonis replied that the procedure was unconstitutional and contrary to the principle of freedom of expression. Most frequently it was the use of the domain name that was illicit rather than the domain name itself.

Marianne Georgelin clarified that, by default, domain names that had been deleted in the month before their re-registration would be suspended. The holder would subsequently be required to prove his their identity and postal address, even if the new holder had no connection whatsoever with the previous one.

Pierre Bonis explained that this was a form of *ex ante* verification, of which there would be very few, the idea being that it should be effective enough to deter any generalisation of *ex ante* verification. Afnic would thus be able to prove effectiveness in detecting cases where the probability of non-compliance was very high. False positives would entail only a slight delay in registration. Incidentally, registrars have the possibility of correcting a number of errors, such as wrong format for telephone numbers. Pierre Bonis insisted on the fact that Afnic's approach was basically one of verification as opposed to prohibition. If the holder is indeed who they claim to be, provided a photocopy of their ID card and proof of address, there was no problem. By way of reminder, several thousand verification procedures are carried out every year. The only new feature introduced in this case is that the domain name will not be published until seven days have passed.

Marianne Georgelin pointed out that the registrar can alter the information during the suspension period (the registrar has the right to correct).

5.3.1. Feedback from the Registrars' and Users' Committees

5.3.1.a. Users

The committee would like to know the number of actions actually taken, not just the number of detections reported. Reachability was an important point raised. And how is validity of a number or an email address determined? Would a short number be authorised? What about disposable, on/off type numbers, much used by fraudsters, but not illegal? Detection work was done on the term "gouv". Does this apply to variants like "qouv"? The impact on an entire portfolio is significant. Does the registry or the registrar telephone the holder before bringing out the big guns and deleting a whole portfolio? The committee had taken due note of the fact that a single element sufficed to trigger an alert. Shouldn't the number be increased in due course?

5.3.1.b. Registrars

The Registrars' Committee was curious as to the reference framework used to check the validity of telephone numbers. It recommended agreeing on a single format with CENTR and the other European registries, so as not to block bundles by adding another extension to the .fr domain. Increasing the number of verifications could also have an effect on pricing. With these verifications it was also important to take account of transfers, changes of holder and the updating of contacts. For example, if a holder is detected by FR Check as having a wrong number and this is then corrected it in order to pass the verification, the particulars will still be wrong if the old number is re-entered two days later. The committee would also like delete commands made at the request of third parties to be identifiable, so that the domain name could be recovered by the rights holder for example. The registrars asked to be informed automatically of requests for verification made. The

committee was minded to apply a weighting to the verifications (legal person status of the holder, registrar with reputation of abuse, etc.).

The committee called for vigilance as to false positives that may have resulting in blocking for using the term “gouv”.

Lastly, two other points had been raised: the possibility of the registrar’s indicating to Afnic that a deletion is linked to abuse; and transmission of the list of abuses via the extranet.

Afnic responded in part to the committees’ questions and observations and indicated that it would examine the rest later.

Pierre Bonis conceded that disposable numbers might generate false positives. Simply put, the aim was to rely on the most objective elements possible so as to leave no room for interpretation. Besides, a domain name would never be deleted without the holder and the registrar first being informed. As a reminder, the period during which the required evidence can be provided is 7 + 30 days in total. Pierre Bonis said he understood users’ concerns, but the verification procedure and FR Check were entirely separate from one another. The number of domain names detected by FR Check was in fact much lower than the number of requests made for verification.

Régis Massé pointed out that 80% of the portfolios associated with a holder comprised only one domain name (cases in which a contact name was identified by domain name were very common).

Pierre Bonis observed that the registrars’ habit of allocating an NIC handle to each domain name was bad practice.

Sébastien Almiron noted that the committees in no way called into question the work done by Afnic. It simply seemed important to stress that the measures proposed were likely to change over time.

Pierre Bonis reaffirmed that when Afnic deleted a domain name, it was because the holder had provided incorrect information. In such cases, all that holder's domain names would be deleted, even if there were 100,000. As already explained, what triggered the procedure was not the domain name but the information relating to the holder. In other words, it was the holder rather than the domain name that was deleted. As regards the suggested weighting, he reminded those present that decisions to delete were not automated. Only redirection to FR Check was automated. When a domain name is deleted at the request of a third party, the rights holder simply has to prove that they are the rightful holder.

Marianne Georgelin explained that if a legal person who already had a portfolio registered a domain name that had been flagged, it was an indication of an intrinsic problem with its particulars. However, they have seven days in which to provide the evidence required, and there is no question of suspending the entire portfolio during this period. For the record, 90% of requests for verification lead to a deletion, thus demonstrating that Afnic does not make many mistakes. If this figure were to fall, one of the criteria would perhaps have to be readjusted.

Régis Massé indicated that the validity of email addresses and telephone numbers was checked using open source libraries (phone number and email validators). Pierre Bonis mentioned the International Telecommunication Union's International Public Telecommunication Numbering Plan for telephone numbers.

Régis Massé clarified that registrars would be informed in due course via API of the verifications under way.

Marianne Georgelin was eager for information from the registrars on deletions due to abuse, since this promoted greater transparency, in line with the recommendations of Arcom, an independent public authority guaranteeing freedom of communication.

5.4. Information on improved detection of abuse thanks to machine learning

5.4.1. Context

Benoît Ampeau explained that it was still not possible to differentiate a legitimate registration from an abusive one with certainty:

- fake data or just a mistake?
- phishing or practice in preparation for phishing?
- typo-squatting or defensive strategy?

5.4.2. There are techniques for calculating risk

Calculation of the risk may focus on the composition of the name:

- mabanque-bnpparibas.fr – **NO**
- mabanque.bonpparibas – **YES**
- notif-laposte.info – **YES**
- paiemet-leboncoin.fr – **NO**

- netflix-compte.fr – **NO**
- comforama.fr – **NO**
- contravention-sncf.fr – **YES**
- ceteleml.fr – **NO**

In other words, the abuse is not always to be found in the composition of the name.

5.4.3. Our approach

An integration chain of different models and tools has been implemented in order to:

- analyse the composition of domain names;
- analyse holders' particulars.

5.4.4. Pipeline of integrated models

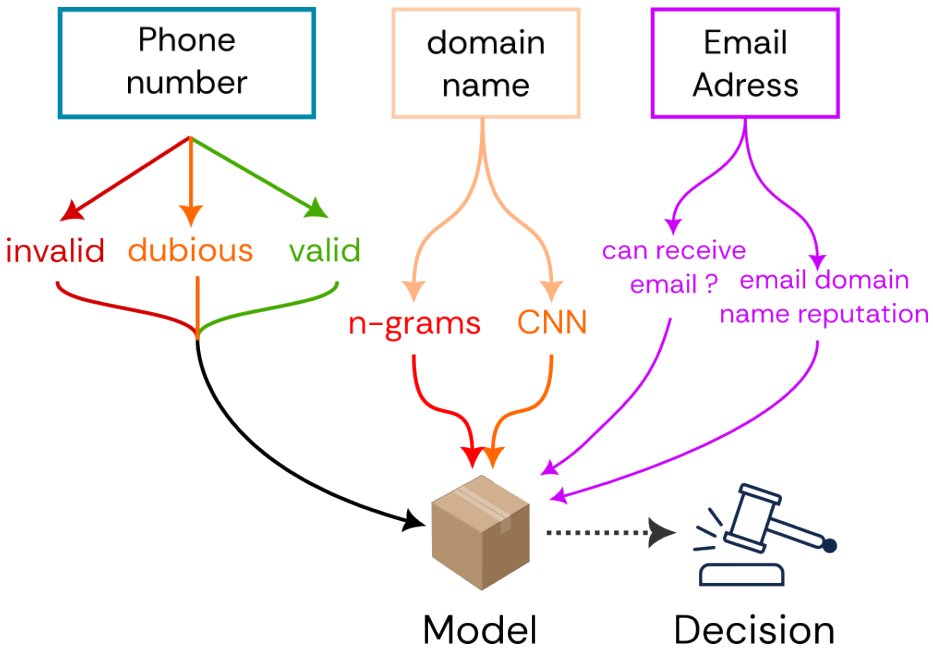


Image Transcription:
The image represents a flowchart illustrating a data validation and categorization process, including phone numbers, domain names, and email addresses.

Here is a detailed description:
1. **Phone Numbers**:
- Phone numbers are evaluated and categorized into three groups: "incorrect" (red), "suspicious" (orange), and "valid" (green).
2. **Domain Names**:
- Domain names are analyzed using two methods: "n-grams" (red) and "CNN" (Convolutional Neural Network, orange).
3. **Email Addresses**:
- Email addresses are evaluated for "reachability" (purple) and "domain categorization" (purple).
4. **Model**:
- The data for phone numbers, domain names, and email addresses are processed by a model (represented by a box at the bottom of the diagram).
- The model produces a final "Result," which is represented by a dashed arrow.
This diagram shows how different data are processed and validated using various algorithms and models to produce a final result.

Taken together, these elements allow us to obtain good results that help Afnic's services to detect abuse.

5.4.5. Progress so far

The software chain tests the results of four complementary modules for the legal teams:

- two on the composition of domain names;
- one on reachability information;
- and one on addresses.

5.4.6. Improved detection of abuse

5.4.6.a. The legal framework

Marianne Georgelin emphasised that, independently of FR Check, Afnic continued to enhance its ability to detect problematic domain names. These detections led to verification procedures being triggered.

Benoît Ampeau confirmed that he received alerts (red flag domains, etc.). Since some abusive practices were not flagged in advance, the aim was to improve detection.

Marianne Georgelin explained that, in introducing processing by machine learning ("Combating abuse"), several purposes were pursued:

- analysis of the naming data in the TLDs managed by Afnic in order to detect domain names used or likely to be used for abusive purposes.
- implementation of automated systems designed to:
    - detect the creation of domain names likely to infringe Afnic's Naming Policy, or to be used to send spam, to set up fake shops, for phishing or to disseminate malware;
    - detect fake or incorrect holder contact particulars (ineligibility, non-reachability);
- initiate and manage procedures, in its capacity as registry, to combat naming abuse.
- draw up statistics and activity reports.

This processing draws on the following lawful bases:

- performance of a task carried out in the public interest (Article 6-1e of the GDPR);

- application of Articles L45-1 and L45-2 of the French Post and Electronic Communications Code (CPCE).

5.4.6.b. Implementation

In summary, the implementation of improved detection of abuse involves:

- automated detection, but with the outcomes being subjected to the same analysis as any other report received by Afnic;

- a non-automated decision: following analysis by the legal department, detection may lead to further action such as a verification procedure or report to the authorities, etc.).

- Updating of holders' data on Afnic's website for information to holders and registrars.

A member of the registrars' college asked whether it was envisaged in due course to check all domain names retroactively with FR Check.

Marianne Georgelin pointed out that, before FR Check was applied to the country code, work had been done to detect domain names with a non-European code. Retroactive checks via FR Check could be suggested in the committee meeting. To recap, the objective was not to be exhaustive, but to improve detection, since abuses normally surface in the first few days after a domain name's creation.

Pierre Bonis stressed that the GDPR constituted an advance in regulation compared with the old "*Informatique et Libertés*" data protection law. Afnic can now work on the purpose of the processing with complete transparency. Indeed, the GDPR is built on the logic of a management system.

6. Calendar of upcoming diary dates

UPCOMING DIARY DATES

- **Thursday 4 December 2025 from 1:30 pm to 3:00 pm:** Webinar – *Report on international bodies*, presented by Lucien Castex
- **Thursday 11 December 2025:** Webinar – *Market trends in domain names*, presented by Loïc Damilaville
- **Tuesday 12 May 2026:** Registrars' and Users' Consultative Committee meetings - Afnic HQ, Guyancourt
- **Wednesday 24 and Thursday 25 June 2026:** Annual sessions of the International College – Afnic HQ, Guyancourt
- **Friday 26 June 2026:** General Assembly at Campus Cyber and Afnic Annual Dinner in Paris

Pierre Bonis thanked all of the participants present both in-person and online for their participation.