DNS IDENTITY

Verification and Authentication of Domain Name
Owners

MAY 2023

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors please use team@enisa.europa.eu
For media enquiries about this report, please use press@enisa.europa.eu.

AUTHORS

Mark McFadden (Plum Consulting, Paris France), Evangelos Kantas (ENISA)

ISBN: 978-92-9204-635-4, DOI: 10.2824/854010

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Domain names and the Domain Name System (DNS) are at the heart of the modern internet. The ability to transform a human-readable string of characters into an Internet Protocol address is fundamental to services and applications that billions of people take for granted. The DNS is also an integral part of reducing spam and locating other services on the Internet.

Domain name registration is the process of registering and configuring a domain name so that it functions properly. As part of this process, the domain name registrant enters into an agreement with the registrar, which includes a requirement for accurate information. The registrar is responsible for establishing verification procedures to ensure that the information collected is accurate and complete, as well as implementing strong authentication controls to guarantee the protection of the accounts related to the domain names.

This report provides a view of authentication and verification of domain name owners in the context of domain name registration. It identifies the security challenges, good practices, security controls and associated risks in the domain name registration ecosystem. It also looks at the risks associated with weak authentication systems and identifies good practices for establishing identity in the context of domain registration.

The first part of the report focuses on the verification of the identity of domain name owners. In particular, it identifies key risks related to the verification process, such as weak passwords, password reuse, and privacy risks, while also categorizes potential attacks on the identity of domain name owners. These attacks are grouped into online vectors – attacks using electronic means – and offline vectors, such as social engineering attacks.

Lastly this first part explores existing good security practice literature on the verification of the identity of domain name owners, including practices from the NIS Cooperation Group, ISO, and ICANN, while it also identifies a list of good security practices, such as:

- support of two-factor authentication (2FA) to strengthen verification,
- use of national eIDS schemes, where available,
- use of PCI DSS data,
- use of third-party verification.

The second part of this report focuses on aspects of authentication of domain name owners. It categorizes authentication techniques, and explores key risk in the authentication process. Finally, this part identifies good security practices on domain name owner authentication. These practices include that registrars, where possible, supplement existing username/password credential systems with 2FA, while also examines advanced approaches to using metadata for authentication in domain name registration accounts.

1. INTRODUCTION

1.1 POLICY CONTEXT

The **Domain Name System** (DNS) is a critical part of the internet infrastructure. It mainly serves as a distributed naming database in which domain names are located and translated into Internet Protocol (IP) addresses. Closely embedded in the functioning of the DNS is **domain name registration**, an essential process of the operation of the internet that involves a registrant acquiring a domain name from a domain name registrar.

This ENISA study on verification and authentication of domain owners aims to provide a view of the security of authentication and verification processes in the context of domain name registration.

1.2 TARGET AUDIENCE AND OBJECTIVES

The target audience of this report are national authorities involved in the security of the DNS, as well as top level domains (TLDs) and entities providing domain name registration services.

The main objective is to give information about possible risks regarding the registration, verification and authentication of domain names, as well as providing good practices on the verification and authentication of domain name owners.

1.3 REPORT STRUCTURE

This report, apart from the introduction and conclusion chapters, is split into two main parts that cover respectively the verification and authentication of domain name owners. In its entirety, the report includes the following chapters:

Chapter 1 – Introduction. The general context, objectives and target audience of the report.

Chapter 2 – Verification of domain name owners. This chapter explores aspects of the verification of domain names owners and includes the following parts:

- Policy context around verification of domain name owners
- The domain name registration process
- Key risks and potential attacks
- Good practices in the verification process of domain name owners

Chapter 3 – Authentication of domain name owners. This chapter investigates aspects of authentication of domain name owners. It includes the following parts:

- Relevant stakeholders in the process of authentication
- Authentication techniques
- Key risks in the authentication process
- Good security practices in the authentication of domain name owners

Chapter 4 – Conclusion. Main takeaways and closing remarks.

1.4 IDENTITY IN THE CONTEXT OF DOMAIN NAME REGISTRATION

For the purposes of this report, a **digital identity** is the unique representation of a subject engaged in an online registration transaction, while **identity proofing** establishes that a subject is who they claim to be. V**erification** is the process of establishing an initial digital identity for the purposes of registering a domain name, and **authentication** is the process of establishing proof of identity for the purposes of managing domain name registrations.

Furthermore, authentication establishes that a subject attempting to access an online registration service is in control of one or more valid **authenticators** associated with that subject's digital identity. For registration services that provide support for return visits, successfully authenticating provides reasonable risk-based assurances that the subject accessing the service today is the same as the one who accessed the service previously.

On this model, a potential registrant applies to a registrar through an enrolment process typically under the control of the registrar. The registrar identity proofs the potential customer, who, if successful, becomes a customer/subscriber to the registrar service. At that point an authenticator (often an email address) and a corresponding credential is created between the registrar and the customer. The registrar maintains the credential, its status, and customer data for the lifetime of the authenticator/credential pair. The customer maintains the authenticator.

Lastly, the classic paradigm for authentication systems, as used in this report, is broken up into three factors:

- something you know (e.g. a password or a personal identification number (PIN)),
- something you have (e.g. an identification (ID) badge or a cryptographic key),
- something you are (e.g. a fingerprint or other biometric data).

AUTHENTICATION FACTORS

Traditional authentication often relies simply on something you know: a password. Many systems are built out of a username (for instance an email address) and a password. Modern systems require two factors to authenticate access to an account.

2. IDENTITY OF DOMAIN NAME OWNERS

2.1 POLICY CONTEXT

2.1.1 Implications of the NIS Directive in verification of domain name owners

In 2016, the European Commission proposed the EU network and information security (NIS) directive[1], the first piece of EU-wide cybersecurity legislation. The goal is to enhance cybersecurity across the EU. The NIS directive was adopted in 2016. As it is an EU directive, each EU member state needed to adopt the legislation in a process called "transposition". The national "transposition" by the EU member states happened on 9 May 2018.

The NIS directive has three parts:

- **National capabilities**. EU Member States must have certain national cybersecurity capabilities, e.g. they must have a national computer security incident response team (CSIRT) and perform cybersecurity exercises.

- **Cross-border collaboration**. Collaboration between EU countries is required, e.g. the operational EU CSIRTs Network and the strategic NIS Cooperation Group.

- **National supervision of critical sectors**. Member States have to supervise the cybersecurity of critical market operators in their country, ex-ante in critical sectors (energy, transport, water, health, digital infrastructure and finance) and ex-post for critical digital service providers (online market places, cloud and online search engines).

For the third of these, ENISA prepared a mapping of security measures for operators of essential services to existing international standards[2] used by operators in the business sectors listed. In particular, the mapping included digital service infrastructures. While the DNS and domain name registration are not within the remit of the report, identity and access management are. In particular, the mapping for authentication and identification points to NIST SP 800-82[3], ISO 27019[4] and NERC CIP[5]. Of these, only the NIST publication has specific language about identification and authentication (in its section 6.2.7).

NIST SP 800-82 makes specific recommendations regarding password authentication, challenge/response authentication, physical token authentication, smart card authentication and biometric authentication. The purpose of NIST SP 800-82 however, is to provide guidance in the

---

[1] "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," https://eur-lex.europa.eu/eli/dir/2016/1148/oj
[2] ENISA, "Mapping of OES Security Requirements to Specific Sectors," January 2018, https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors/
[3] Stouffer, K., Pilitteri, V., Lightman, S., Abrams, M. and Hahn, A., "Guide to Industrial Control Systems (ICS) Security", National Institute os Standards and Technology, 2015, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
[4] ISO/IEC, "Information Technology - Security techniques - Information security controls for the energy utility industry," 2019, https://webstore.ansi.org/Standards/ISO/isoiec270192017
[5] NERC, "NERC (CIP) Critical Infrastructure Protection," https://www.nerc.com/pa/comp/guidance/Pages/default.aspx

context of industrial controls and not general access to secured applications (such as a management tool for domain name registration management).

In Article 4 (4), the NIS directive states: "'operator of essential services' means a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2)". Annex II includes a section on digital infrastructure, which includes both DNS service providers and TLD name registries. In fact, the language of the NIS is clear about the fact that the security requirements of these services are essential: "Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services" – Article 14(2).

However, other than listing DNS service providers and TLD name registries as being subject to its requirements, the NIS directive, the act makes no further specific mention of them.

2.1.2 The NIS 2 directive

On 13 May 2022, the European Council and Parliament approved the initial proposed text for a "Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union[6] (NIS 2)". At the time of completion of this report, the final NIS 2 text was not available. In alignment with the first NIS directive, it is broken into two main parts: the articles containing the provisions of the law, and a pair of annexes containing a list of the entities subject to the law's provisions. The stated goal of the directive is to enhance cybersecurity capabilities across the Union, while mitigating threats to network and information systems used in essential services and ensuring the continuity of such services in the face of cybersecurity threats.

The NIS 2 article specific to this topic is titled "Database of domain name registration data". Most of this article discusses domain registration data and not specifics related to the verification or authentication of domain name owners. For instance, paragraph (3) states that Member States shall require the TLD name registries and the entities providing domain name registration services have policies and procedures, including verification procedures, in place to ensure that the databases include accurate and complete information.

The remaining parts of the article discuss requirements for publication of the registration data and access to that data.

2.1.2.1 Jurisdiction and domain name registration in NIS2

NIS2 has a broad view of its jurisdiction. This feature is important in the context of domain name registration services. The relevant article of the proposed NIS 2 text, "Jurisdiction and Territoriality", is devoted to this topic and states that, if an entity in the scope of the directive is not established in the Union but offers services within it, it must designate a representative established in one of the Member States where services are offered and shall fall under the jurisdiction of that Member State.

Many DNS name registration services offer services throughout Europe, while several others operate global name registration services. In either case, it is apparent from the language of the article related to jurisdiction that NIS 2 does apply to DNS name registration services, even if those services are provided by a company outside the European Union. In order to tell if the domain name registration service comes under the jurisdiction of NIS2, the proposed text of the act provides the following guidance:

> "In order to determine whether such an entity is offering services within
> the Union, it should be ascertained whether it is apparent that the entity

---

*is planning to offer services to persons in one or more Member States.
The mere accessibility in the Union of the entity's or an intermediary's
website or of an email address and of other contact details, or the use of
a language generally used in the third country where the entity is
established, is as such insufficient to ascertain such an intention.
However, factors such as the use of a language or a currency generally
used in one or more Member States with the possibility of ordering
services in that other language, or the mentioning of customers or users
who are in the Union, may make it apparent that the entity is planning to
offer services within the Union."*

In any case, it is clear that global and regional name registration services offering services in the
EU are, by definition, under the NIS2 cybersecurity mechanism. NIS2 reflects this in guidance
that the cybersecurity requirements for companies providing DNS-related services (DNS name
registries in particular) should be harmonized at EU level.

2.1.2.2 Domain name registration security and NIS 2

NIS2 requires, at a minimum, the following data to be collected as part of the registration
process: the domain name itself, the date of registration, and basic information about the
registrant. NIS2 requires that the as part of the registration activity, there are policies and
procedures in place to ensure that accurate and complete information is kept and that those
policies and procedures are made public.

As a result, NIS 2 places a requirement on any company offering domain name registration
services. That requirement includes a data collection component, a validation component and a
publication component. Data collection and validation are key components of identity
management. However, publication of the data is not a key component, and will not be
discussed further.

NIS 2 therefore requires that every registration have a minimum set of data collected, validation
of that data, and publication of the policies and procedures that ensure that the data is accurate
and complete.

As we will see further below in the report, the process of initial domain name registration
involves establishing a contractual relationship between registrant and registrar. The registrar
acts as a service point for the registrant and effectively collects contact and billing information.
Since almost all transactions between registrant and registrar involve the exchange of money
for services, validation and approval of the data is often completed by a third-party on behalf of
the registrar (for instance, a credit card processing provider). Thus, the registration mechanisms
would meet the requirements of NIS 2.

In addition, ongoing renewal of domain names – described further below, in Section 2.2.3 –
would also meet the requirements for NIS 2.

However, ongoing maintenance of the domain name registration information – described below,
in Section 2.2.3 – might not meet the requirements of NIS 2. If a registrant used their credentials
to change the data related to their registration, but did not invoke a process such as payment
authorization, the result could be inaccurate information in the registration database without a
mechanism to validate that data. In order to be compliant with NIS 2, the registrar would have to
invoke a secondary mechanism for validation of that data.

2.1.3 ICANN contractual requirements

For gTLDs, there are more than 2000 ICANN accredited registrars and resellers. Registrars for
gTLDs are accredited by ICANN and certified by registries to sell domain names. Since 2013,

the registrars have been bound by a Registrar Accreditation Agreement (RAA)[7] with ICANN and by contractual agreements with individual registries. Resellers are organizations affiliated with or under contract to registrars to sell domain names and offer related services such as web hosting and email. Resellers are bound by the contractual agreements they have with the registrars and are not accredited by ICANN. The registrars remain responsible and accountable for all domain names sold by associated resellers.

For ccTLDs, these contractual requirements do not apply because almost all ccTLDs do not have a contractual relationship with ICANN. This is important because the registry operator for the ccTLD is often the organization that collects the registration data (instead of a registrar).

Part of the RAA specifies the data that need to be exchanged between the registrar and the registry. Some of the information transmitted between the two is specific to the business relationship between the specific registrar and the registry operating the TLD. The six requirements in the RAA are:

1. the name of the Registered Name being registered,
2. the IP addresses of the primary nameserver and secondary nameserver(s) for the Registered Name,
3. the corresponding names of those nameservers,
4. unless automatically generated by the registry system, the identity of the Registrar,
5. unless automatically generated by the registry system, the expiration date of the registration,
6. any other data the Registry Operator requires be submitted to it.

The contract also requires that the registrar collect a series of data items that support a public query facility. The contract has the following eight requirements:

1. the name of the Registered Name (domain name),
2. the names of the primary nameserver and secondary nameserver(s) for the Registered Name,
3. the identity of the registrar (which may be provided through the registrar's website),
4. the original creation date of the registration,
5. the expiration date of the registration,
6. the name and postal address of the Registered Name Holder,
7. the name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the Registered Name,
8. the name, postal address, e-mail address, voice telephone number and (where available) fax number of the administrative contact for the Registered Name.

Four of these requirements overlap with the contractual obligations for communication between registrar and registry. It is the registrant who has contractual responsibility for the accuracy of the above information, and wilful failure to provide accurate information results in a breach of the relationship between the registrant and the registrar. However, the WHOIS Accuracy Program Specification requires the registrar to verify only the email address or telephone number of the Registered Name holder[8].

It is worth noting that the RAA does not specify authentication practices. In particular, the it does not specify that registrars should use authentication technology stronger than userID/password approaches.

---

[7] https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en
[8] In Section 1.f of the WHOIS Accuracy Program Specification, the registrar is given guidance on how to go about doing this validation. It is also worth remembering that many ccTLDs do not have a formal relationship with ICANN and, as a result, the WHOIS Accuracy Program is entirely optional for them.

2.1.4 ICANN policy requirements

The RAA is specific about the responsibilities of registrants in regard to domain name registration. The registrant:

- must comply with the terms and conditions posted by the registrar, including applicable policies from the registrar, the registry and ICANN;
- must review the registrar's current registration agreement, along with any updates;
- will assume sole responsibility for the registration and use of the chosen domain name;
- must provide accurate information for publication in directories such as WHOIS, and promptly update this to reflect any changes;
- must respond to inquiries from the registrar within 15 days, and keep the registrar account data current; if the domain name registration renews automatically, the registrant must also keep their payment information current.

2.1.5 ccTLDs and gTLDs

Before proceeding to the next section, it is important to clarify the distinction between ccTLDs and gTLDs.

gTLDs are called generic for largely historical reasons. They represent a variety of interests from truly global, widely accessible domains such as .com, .net or .org. Geographic TLDs represent the interests of a specific geographic location or region. Brand TLDs are used by particular companies in promotion of their brands. Finally, restricted TLDs serve a particular interest group or set of stakeholders. The rules for registration, including how verification and authentication are done, are specific to the registry for that TLD.

ccTLDs are TLDs reserved for a single country, sovereign state or dependent territory. The ccTLDs are two letter codes based on ISO 3166-1. The registration policy, including verification and authentication of domain owners, is specific to each ccTLD and varies widely throughout the world.

2.2 THE DOMAIN NAME REGISTRATION PROCESS

2.2.1 Stakeholders and roles in domain name registration

2.2.1.1 Registrants

A domain name registrant is an individual or entity that registers a domain name. When the registrant registers a domain name, they enter into a contractual relationship with a registrar. The contract describes the terms under which the registrar agrees to register and maintain the requested domain name. Once the domain name is initially registered, registrants manage their domain name and its configuration through tools provided by the registrar.

2.2.1.2 Registrars

A registrar is an organization that allows individuals and entities (registrants, see 2.2.1.1 above) to register domain names. During the registration process, the registrar verifies that the requested domain name meets the policy of the registry operator and then submits the name and other required information to the registry operator. Registrars also are required to collect information form registrants and make that information available publicly. After registration, registrants can make updates to their domain name configuration through tools provided by the registrar. Registrars are able to sell domain names for many TLDs and have contractual arrangements with each of those TLDs.

2.2.1.3 Registries

A registry operator is a company that keeps an authoritative database of the domain names registered in a TLD. Each TLD in the DNS is associated with a registry that contains a record for every domain name that exists in its domain. The DNS uses the TLD registry to obtain the names of the authoritative name servers for all the domain names registered in that TLD.

Registry operating models

There are three operating models in play in Europe:

- the registry/registrar model, in which the registry only offers management of the zone file and related information associated with the TLD, and registrations and domain name management are done by registrars,
- the direct registration model, in which the registry works directly with the registrants and bypasses the registrar role (for instance .dk, .de and .es)[9],
- the hybrid model, in which the registry accepts domain name registrations both indirectly, from registrars, and directly from individual users (for instance .cy and .at).

2.2.1.4 Resellers

A domain name reseller is a third-party company that offers domain name registration services through a registrar, but not all are registrars accredited with the Internet Corporation for Assigned Names and numbers (ICANN). There are additional requirements for resellers of registrars under the 2013 Registrar Accreditation Agreement (RAA), including web posting obligations, disclosure requirements and oversight by registrars.

2.2.1.5 Policymakers and regulators

As seen from the brief overview of the NIS Directive and the proposed text of NIS 2 (in section 2.1.2), policymakers and regulators have a role to play in ensuring stability, security, privacy, and market fairness in the registration ecosystem. Internet governance is beyond the scope of this report, but ICANN supports bottom-up, multistakeholder policy development in a context where governments have a direct role through the Governmental Advisory Committee (GAC).

GAC advice has a particular status under the ICANN ByLaws. Its advice must be duly considered by the ICANN Board, and when the board proposes actions inconsistent with GAC advice it must give reasons for doing so and attempt to reach a mutually acceptable solution. However, ICANN is primarily concerned with the technical administration of the DNS namespace.[10] While verification and authentication of registrants is a topic of concern to ICANN, governments and policy makers have recently been looking outside the boundaries of ICANN to have an influence on the security of the registration ecosystem.

Policymakers also find themselves addressing security and stability issues in the cases where a registry operator has no contractual arrangements with ICANN (country code top-level domains (ccTLDs)). In these cases, security and stability issues – and verification and authentication of domain name owners – are a national matter and are addressed by the government and the local organization that proves the registry services for the ccTLD.

---

[9] The model, in which a country code top-level domain (ccTLD) directly serves registrants is important. In many countries the ccTLD registry operator is embedded in national governmental entities. This influences the policies and procedures under which registrations can be made and also how pan-European initiatives are implemented. Generic top-level domains (gTLDs) follow a different model and are largely transnational. This has an implication for how proposed legislation, such as the proposed revision of the directive on the security of network and information systems (NIS 2), is incorporated in different countries' national laws.

[10] It has other roles in addressing and supporting the Internet Assigned Numbers Authority.

2.2.2 How domain name owners are identified upon initial registration

To begin the process of registering a new domain name, a registrant chooses a registrar, choses an available domain name and then enters into an agreement with the registrar to have the domain name managed and placed into operation by a registry operator. There have been more than 4,000 registry operators counting both those that are currently active and those that have had their agreement with ICANN terminated[11].

The relationship between registrant and registrar is almost always mediated by a web-based set of management tools. In order to complete an initial registration, there are two common approaches:

- the registrant creates an account and then uses that account to select, configure and pay for new domain names,

- the registrant first selects the domain names and then provides identity information as part of the billing process for that domain name.

The first case is far more common for registrars that provide services to European registrants. In creating an account with the registrar, a small number of registrars allow the user or entity to use the credentials established at another organization as the means of establishing identity for the registrar. This uses the protocol called OAuth 2.0[12]. OAuth 2.0 allows the user to use credentials from other sites (such as Facebook, Google or Apple) to establish identity at the registrar.

Using this strategy, the registrar is able to collect information on and market to a larger community than if only customers were part of the contact database. By far, most registrars serving Europe use this approach and collect only an email address and a password. In no case did this study find alternative identification technologies in operation for initial contact with the registrar.

In the second case, the registrar establishes a relationship with the customer only if they actually acquire a domain name. In this case, the registrar can acquire significantly more information about the registrant as part of the billing for the domain name. For example, by waiting until the customer enters billing and payment information before establishing an account, a registrar using this approach has far more information available at the time the account is set up.

In a very limited number of cases, other tools are used to protect the account sign-up process (e.g. Captchas or supplying a tax or phone number).

During the desktop research, the prevalent way of establishing initial contact with registrants is without ordering a domain name, as shown in the graph below.

---

[11] See https://www.iana.org/assignments/registrar-ids/registrar-ids.xhtml
[12] See https://oauth.net/2/

Figure 1 - How are identities established at registrars?
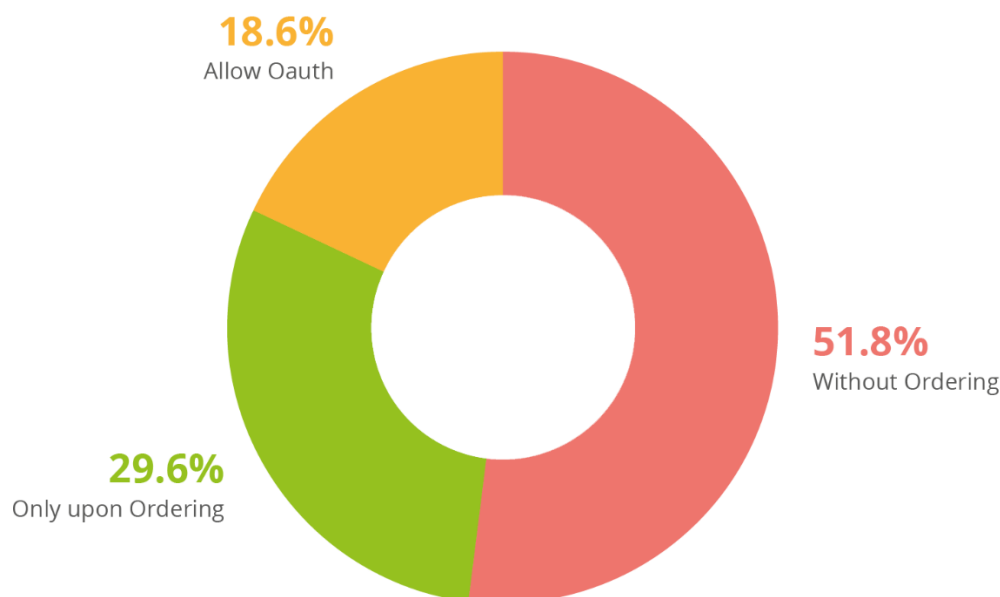
In all three cases, registrars get the most detailed information about the domain name owner during the process of purchasing the registration service. In the ordering and billing steps of the acquisition, the registrant must provide enough information to support publication of WHOIS information related to the domain name as well as to allow the financial transaction to be successfully completed. Upon initial registration the registrar has access to:

- information about the location (postal and physical) of the registrant;

- information needed to support approval of financial transactions (particularly, but not limited to credit card related information);

- a working email address for contacting the registrant; and

- in some cases, related information such as tax numbers, PINs for contacting support, demonstrations that the domain was not initiated by a robot, and other information collected as part of the initial registration.

It is important to note that the information here is subject to applicable regulations such as the EU's general data protection regulation (GDPR). The registrar may collect information related to identity, but the rules for publishing those data are very complex[13].

2.2.3 Identity management at renewal and ongoing maintenance

Previously in the report, the two components of initial registration were discussed: establishing a relationship (including an online account) between the registrant and the registrar, and ordering and purchasing the domain name.

---

[13] Registrars must balance privacy and personal data concerns against legitimate third-party interests, such as addressing legal disputes. This especially affects the availability of contact information in public WHOIS databases.

Importantly, the two are tied together for the life of the relationship between domain name, domain name owner and the registrar.

Once this relationship has been established, the domain name is put into operation. This does not mean that the information exchanged in the initial process is unchanging. Instead, the domain name owner needs to maintain the information throughout the life cycle of the domain name. Authoritative servers, mail servers, other DNS resource records and contact details may change throughout the lifetime of the domain name. The authoritative contact for those records must have the ability to maintain those records.

In all but a few cases, the maintenance of the domain name information is done through a web-based management interface. The maintenance tools provide the registrant with access to all supported configuration options that they can change without manual intervention by the registrar.

Using the web-based interface requires that the registrant provide credentials that identify them to the registrar. In every case, this is the account information established when the registrant first originated a relationship with the registrar or when they made their first order of a domain name. In the cases where the registrant uses OAuth as a tool for authentication, they are allowed to continue to use OAuth for ongoing maintenance.

It is important to note that web-based maintenance of domain name records is not the only approach available to registrants. Many registrars provide phone-based services so that registrants can contact a registrar and speak directly with a customer service representative. In these cases, the registrar has access to all the information related to the registrant's account (not just the userID/password credential). It is then possible to use the other, related information as secondary sources to verify the identity of the domain name owner during a support call.

Domain name ownership has a lifetime: commonly 1, 2 or 3 years (but sometimes as much as 10 years). In order to continue using the domain name after its original lifetime, the registration must be renewed. Renewal allows the registrant to continue using all the features of the domain name without interruption. Renewal is almost always a feature of the web-based management tools that are available to the domain name registrant. The mechanism for establishing identity for renewals, in these cases, is exactly the same as for all other features of the domain name maintenance user interface[14].

2.2.4 Identity management in domain name transfers

It is the right of all registrants to transfer a domain name registration between registrars[15].

The process of transferring a domain name from one registrar to another is more complicated than simply acquiring a single domain name. The process begins by having the customer initiate a relationship with the new registrar (called, the "gaining" registrar). The gaining registrar continues the process by sending the registrant a form that is used to confirm the registrant's intention to move the domain name. The information in that form is used to notify the previous registrar of the transfer request.

Identity management during domain name transfers requires that the registrant have accounts at both of the registrars involved (both the gaining and the losing registrar). In addition, a losing "auth-code" (also called an Authorization Code, AuthInfo Code, Auth-Info Code, or transfer code) is a code created by a registrar to help identify the domain name holder and prevent

---

[14] In an extremely small number of cases – two – we found that registrars serving European customers required renewals to be done through a phone call to customer support rather than through the web-based interface. As a proportion of the full set of registrars, this number is vanishingly small. We believe that these registrars used this strategy to attempt to sell the registrant add-on services.
[15] See https://www.icann.org/resources/pages/transferring-your-domain-name-2017-10-10-en

unauthorized transfers. An Auth-Code is required for a domain holder to transfer a domain name from one registrar to another.

The losing registrar may allow the registrant, via the online interface described in Section 2.2.3 above, to generate and manage their own AuthInfo code for the transfer. In a limited number of cases, the registrants will need to contact their registrar directly to obtain it. The registrar must provide their registrant with the AuthInfo code within five (5) calendar days of a legitimate request.

The registrar may ask the registrant for an authorization code to help ensure the identity of the person making the transfer request.

2.3 KEY RISKS AND POTENTIAL ATTACKS

2.3.1 Trust relationships during initial domain registration
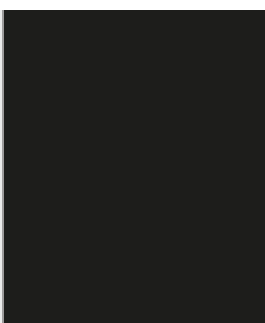
A trust framework is a set of rules and policies that govern the relationships between the key participants in domain name registration. Those rules and policies include (but are not limited to):

- conducting identity management responsibilities;
- sharing identity information;
- using identity information that has been shared with them;
- protecting and securing identity information;
- performing specific roles within the federation;
- managing liability and legal issues.

Table 2, below, shows the trust relationships in place during the initial registration of a domain name.

Table 1 - Trust relationships during initial registration of a domain name

Entities	Registrants	Registrars	Registries
Registrants		Registrants trust registrars with personal details including personal, technical, billing and payment information. Registrants trust that needed and appropriate information will be forwarded to registries to complete the domain name registration process.	Registrants trust registries to accurately publish information needed for a chosen domain name to appear active in the DNS with appropriate configuration and security information as supplied by both the registrant and registrar.
Registrars	Registrars trust and verify registration data needed for both use by the registrar and the data needed to complete the domain name registration with the registry. Registries verify and then trust payment information from the registrant.		The trust relationship between registrars and registries is contractual and spells out the mechanisms (EPP) by which a registry converts its records from a successful registrant registration into information that the registry will use to publish in the DNS.

Registries	Registries have a limited trust relationship directly with registrants except in the cases where they act as both registry and registrar (for instance, in the case of many ccTLDs). In those cases, the trust relationship between registries and registrants is the same as that between registrars and registrants.	The trust relationship between registries and registrars is contractual. The registry operator trusts the registrar to ensure that the information capture in the initial registration of the domain name is accurate and specifies levels of assurance for that information.	

2.3.2 Risks and potential attacks on registrants

Credentials are an essential part of domain name registration. Registrants, resellers and agents use credentials to log into systems to purchase, configure and maintain registrations. Attacks on the credentials result in problems with domain hijacking, traffic interception, social engineering attacks and others.

Some recent examples of these kinds of attacks include the "Onamae.com" attack of May 2020 leading to the hijacking of the crypto domain Coincheck[16], and the "Webnic.cc" attack of February 2015 which led to the hijacking of the domain name of the computer maker Lenovo.com[17].

Registrants are either individuals or entities that register domain names. When a domain name is registered, the registrant enters into a contractual relationship with either a registry operator or a registrar. Some registries allow direct registration of domain names, bypassing the need for registrars in the ecosystem. The contract that the registrant enters into describes the terms and conditions under which the registrar agrees to register and maintain the chosen domain name.

There are several ways in which a registrant can enter into such a contract:

- by establishing a relationship with a registry that also acts as a registrar;
- by establishing a relationship with an ICANN accredited registrar,
- by establishing a relationship with a registrar accredited by a ccTLD, or
- by establishing a relationship with a reseller of registrar services.

In almost all of these cases, the registrant is given web-based account management tools to allow them to register, renew and maintain their domain names. The management tools also allow the registrants to add value added services in addition to the domain name services (these often include web and email hosting, TLS certificates, virus and malware protection, and other services).

The account management services require the registrant to authenticate themselves prior to accessing the tools that allow for maintenance of the account. In the vast majority of cases in Europe, for both ccTLDs and generic top-level domains (gTLDs), the authentication is based on a combination of identity string and password.

---

[16] Baker, Paddy, "Coincheck Customers Fall Victim to Data Breach After Domain Account Error," Coincheck, 3 Jule 2020, https://www.coindesk.com/crypto-exchange-coincheck-victim-domain-data-breach
[17] Krebs, Brian, "Webnic Registrar Blamed for Haijack of Lenovo, Google Domains," Krebs on Security, 26 February 2015, https://krebsonsecurity.com/2015/02/webnic-registrar-blamed-for-hijack-of-lenovo-google-domains/

Using a user identifier and password is extremely common in the domain name registration ecosystem, but it is also subject to clear risks and attack vectors[18].

2.3.2.1 Typical attack scenarios for registrars and Registrants

The Open Web Application Security Project (OWASP) gives three typical attack scenarios that potentially affect registrars and the identity management systems they use:[19]

> *Scenario #1*: Credential stuffing, the use of lists of known passwords, is a common attack. Suppose an application does not implement automated threat or credential stuffing protection. In that case, the application can be used as a password oracle to determine if the credentials are valid.
>
> *Scenario #2*: Most authentication attacks occur due to the continued use of passwords as a sole factor. Once considered good practices, password rotation and complexity requirements encourage users to use and reuse weak passwords. Organizations are recommended to stop these practices per NIST 800-63[20] and use multi-factor authentication.
>
> *Scenario #3*: Application session timeouts aren't set correctly. A user uses a public computer to access an application. Instead of selecting "logout", the user simply closes the browser tab and walks away. An attacker uses the same browser an hour later, and the user is still authenticated."

2.3.2.2 Phishing/sniffing/keylogging

One of the easiest ways to attack the userID/password authentication system is to simply have the registrant provide the credentials to the attacker. Social engineering remains the most prevalent attack vector for attacks on network resources[21]. One attack approach is to trick the registrant into typing the credentials into malicious websites under the control of the attacker. This is an attack strategy called phishing[22]. A recent report shows that up to 32% of employees click on phishing emails, a percentage that indicates how dangerous and effective this attack type is[23].

Another approach to having the registrant disclose the userID/password combination is to have it travel over an insecure, unprotected or unencrypted network. Attackers can use passive attacks on networks that collect and analyze packets as they pass through transmission media. If the account details are passed in cleartext, the attacker can capture the credentials without the knowledge of the registrant.

Another approach is to install either a device or a piece of software that logs all activity on a computer. All keystrokes – including the userID/password combination – can be captured. This strategy works even when the communication channel between the registrant and registrar is encrypted.

2.3.2.3 Brute force attacks

Brute force attacks on credentials use automated tools and dictionaries to generate billions of potential passwords and then try them against individual userIDs. The attacker will examine a website's rules for generating a valid password at a website and then use automated tools to try combinations of letters, numbers and symbols that abide by the password rules.

---

[18] In 2018, hackers stole 500 million personal records, an increase of 126% on the previous year, Cyprus Data Defense, "6 password security risks and how to avoid them," https://www.cypressdatadefense.com/blog/password-security-risks/
[19] "A07:2021 – Identification and authentication failures," OWASP Top 10: 2021, https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/
[20] Grassi, Paul, Garcia, Michael and Fenton, James, "Digital Identity Guidelines," National Institute of Standards and Technology, 2017 and 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
[21] Verizon, "2021 Data Breach Investigations Report," https://www.verizon.com/business/resources/reports/dbir
[22] ENISA, "ENISA Threat Landscape 2021," https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
[23] Statista, "Employees that click on phishing emails in 2020, by age", https://www.statista.com/statistics/1253420/employee-clicks-phishing-emails-by-age/

Brute force attacks are generally easy to prevent online. It is common for authentication systems to have a bad password attempt limit, whereby a user is given a finite number of attempts to enter the correct combinations of userID and password.

However, brute force attacks are very successful in cases where the attacker has access to the system's password file, a list of userIDs and hashed passwords or a database of hashed passwords for the system. If the attacker can gain access to one of these resources, executing the attack offline can make it easy to identify correct combinations of userIDs and passwords.

Attackers have wide access to huge "dictionaries", which are enormous lists of commonly used words and strings with character substitutions, changes in languages, and information gleaned from other, successful attacks. When a system stores password insecurely, the combination of trying many potential passwords against the stored hashes can easily compromise many accounts.

Another type of brute force attack targets the hashed versions of the passwords instead of the passwords themselves. An attack that attempts to crack a hashed password by comparing it with a database of pre-determined password hashes, known as a rainbow table.

A rainbow table takes frequently used passwords, hashes them using common hashing algorithms and stores the hashed password in a table next to the plaintext password. If the attacker gains access to a database that contains hashed passwords, they can compare the stolen hashes to those that are pre-computed in the rainbow table. If any of the hashes match, then they will know the original plaintext password.

2.3.2.4 Weak passwords

Registrants need to create userID/password combinations to gain access to domain name management tools. Relying on a user to generate a password often results in a password that takes on the characteristics of some memorable or meaningful detail that is simple in structure. A balance between memorability and security is often difficult to achieve. Application and systems administrators want passwords that are unpredictable, frequently changed and specific to the system being secured. Users want passwords that are simple and easy to remember.

User generated passwords tend to include patterns that include the meaningful details that make the passwords easy to remember. However, attackers understand these patterns as well. Weak passwords are also particularly vulnerable to dictionary-based brute force attacks.

2.3.2.5 Reuse of existing or compromised passwords

For any user, once one account is compromised, all of the accounts that share that same password become compromised as well. As a password is repeatedly reused, the number of opportunities for exploiting a compromise of that password increases. In settings outside the registration ecosystem, when a website or app is compromised, attackers will use the passwords and login information on other websites in attempt to gain access to other services such as financial websites or email websites.

The fundamental problem is that individual users or entities have an average of more than 100 different accounts. Asking users to use strong, unique passwords for all their accounts is difficult in practice. Password management and generation tools exist in the marketplace, but recent surveys show that fewer than 30% of all users take advantage of software-based tool to create, manage and use strong and unique passwords.

Research also shows that 73% or online accounts use duplicated passwords[24]. The same research shows that more than half of consumers (54 percent) use five or fewer passwords across their entire online life, while 22 percent use just three or fewer. More than half of those surveyed were unfamiliar with multi factor authentication (MFA).

2.3.2.6 Fraudulent registration attacks

In this case, the attacker attempts to abuse the registration account creation process to create fraudulent accounts. The threat to the registrar can be harm to the registrar's ability to deliver registration services because the namespace for legitimate registrants is exhausted. If the registrar provides something of value at the time of registration, fraudulent accounts can be used to harvest awards or incentives that are associated with initial account creation.

A common approach is for the attacker to use a botnet to attempt to automate the creation of thousands or more accounts. The attacker can use available lists of common user names to assist in the creation of bogus accounts. The impact to the registrar can be lost of legitimate customers, reputational damage and operational costs associated with cleaning and deleting the bogus accounts.

2.3.2.7 Abuse of password recovery/reset systems

A key vulnerability of authentication systems is the ability to help "remember" or reset a password. With more than 100 accounts per person to secure, it is natural that people occasionally forget their passwords. Many applications and authentication systems provide a facility for either resetting or recovering the password.

However, that same application tool is an attack vector for the userID/password credential pair. Older systems provided a set of "secret questions", which, when answered, allowed the user to change or reset the password. These systems sometimes relied on questions involving birthdays or maiden names that could be reasonably looked up in other services (e.g. social media). Worse yet, these generic questions are often re-used across applications and services meaning that, if compromised in one place, they lead to the same risks as we have seen previously in the reuse of existing passwords.

2.3.2.8 Cleartext exchange/storage of passwords

Another attack is the examination of code, configuration files, and other supporting files that may have credentials embedded in them. If the credentials are embedded in plaintext, they are simple to extract and exploit. Embedded credentials in plaintext have been seen in HTML code, configuration files and executable code where a developer is attempting to provide access to a protected resource. A good practice here is to have those passwords, if they need to be in configuration files, stored in an encrypted version. An even better practice is to not have passwords embedded at all in configuration files or code.

Automated password fillers, such as those in Chrome, Firefox and Edge also have a similar risk. Auto-filling is when a password manager or browser fills in the username and password fields in a website's login page with a user's saved credentials without the user actively prompting the password manager. The characters automatically pasted into the field can then be "read" by scripts present in the login page — such as might be preset in an online ad that has nothing to do with the page itself — and those scripts will be able to copy and send the username and password anywhere.

[24] Telesign, "Telesign Consumer Account Security Report", 2021, https://www.telesign.com/resource/telesign-consumer-account-security-report

By creating invisible "login scripts", the attacker can create fields that capture credentials without the user's being aware. For registrants and registrars, the vulnerabilities of cross-site scripting need to be avoided to keep verification and authentication secure[25].

2.3.3 Privacy risks related to the identity of domain name owners

Under European and member state law, personal data on domain name holders collected in domain name services include:

- name;
- where available, personal identity code / other personal identifier;
- postal address;
- telephone number;
- contact person and phone number of contact person (legal persons);
- email address (electronic address for service).

Registrars are responsible for ensuring that these details are up to date. If a registrar collects non-statutory data on a domain name holder (for instance DS record for DNSSEC, name servers in use for the domain name or sponsoring registrar), the registrar acts as the data controller of those non-statutory data under the GDPR. In Europe, registrars must maintain a privacy policy covering their processing activities (see Article 30(2) of the GDPR).

Information collected as part of the registration process has historically been published in a database called WHOIS. Publication of personal information has been the subject of volumes of public policy, technical, legal, and regulatory analysis, and remains, to this day, a dilemma for those using the registration system[26]. In fact, as far back as 2003, European data protection authorities have regularly taken issue with WHOIS.

Despite a number of efforts to update WHOIS policy, and to design solutions that meet privacy needs while preserving access for legitimate purposes, the system has remained relatively unchanged.

While WHOIS is continuing source of controversy, and so is the attempt to develop a unified model for continued access to full WHOIS data, its connection to verification and authentication is limited to the fact that WHOIS data is captured or generated in the domain name registration process. In particular, the verification of data used for initial registration is an essential component of the attempt to provide accurate registration information for uses beyond the operation of the DNS[27].

2.3.4 Potential attack vectors related to the identity of domain name owners

Attack vectors related to identity go beyond the traditional security defence-related vectors (such as ports, protocols or services). Instead, attack vectors can be digital, physical and even social. Fundamentally, a threat actor wants to compromise an identity and use it for their own malicious intent. If the identity is a privileged account, then the risks are significant. The goal of the attack is to impersonate a person in the ecosystem at the highest level of privilege possible and then use those credentials as far down the account chain as possible.

---

[25] "No boundaries for user identities: Web trackers exploit browser login managers," Gunes Acar, Steven Englehardt, and Arvind Narayanan, Freedom to Tinker, https://freedom-to-tinker.com/2017/12/27/no-boundaries-for-user-identities-web-trackers-exploit-browser-login-managers/
[26] A typical WHOIS record is shown in Annex B.
[27] For instance, legitimate law enforcement, dispute resolution and remediation of domain name abuse.

Based on ICANN's SAC 40[28] and its observations about domain name registration incidents, vectors for attacks on the identity of the registration ecosystem can be divided into two groups:

- **electronic vectors** (online risks), in which the attacker uses traditional digital methods to impersonate a legitimate user,

- **offline vectors**, in which the attacker uses physical – rather than digital – methods to impersonate a legitimate user.

Electronic methods can include vulnerabilities and exploits against software flaws that can result in exploitation and ownership of an account. These methods also include misconfigurations of software that allow hijacking or the improper creation of registration-related accounts. This group of methods also includes credential and password attacks that give a threat actor unintentional access to registration-related accounts.

Physical methods (social/non-online risks) include supplying falsified documentation, social engineering attacks, and theft and malicious implementation of biometric data.

2.3.4.1 Online vectors

Based once more on observations from ICANN's SAC 40, the most vulnerable attack vector is the account set up between the registrant and registrar to control an organization's, or individual's, domain name portfolio. This is almost always a user account name (email address) and password.

Another online risk is related to the domain name registration online service itself. Attackers scan domain account registration and administration portals for well-known application vulnerabilities (e.g. SQL injection). A successful exploit against vulnerable application code at the registration site can result in the disclosure of the credentials of many domain name registration accounts.

Email is a further attack vector for domain name registration accounts. Email is often the only mechanism used to communicate between the registrant and the registrar about registration activity. Access to the email channel or diversion of messages leaves the registrant unaware of potential changes to registration information. It is possible to also completely block delivery of any email to registrants through unauthorized modification to the MX or other records in the registration.

Recovery from malicious activity in the domain name registration system is almost always a long process, and correcting information that has been globally distributed throughout the DNS can take substantial amounts of time because of way DNS records are distributed to recursive DNS resolvers.

Another attack vector is a denial-of-service (DoS) attack on the registration system itself. By removing the availability of the domain name registration management system, the attacker is able to prevent legitimate users from changing or updating legitimate information in the registrar database. The result is that an attacker could coordinate the DoS attack vector with an attack on domain name registration accounts, making recovery temporarily impossible.

2.3.4.2 Social / offline vectors

The account name/password combination is also subject to attack from non-online vectors such as guessing, social engineering and database attacks.

Just as in other network-based applications, threat actors use social engineering techniques to conceal their true identities and motives, presenting themselves as trusted individuals or

---

[28] "SAC 40 Measures to Protect Domain Registration Services Against Exploitation or Misues," ICANN SSAC, August 2009, https://www.icann.org/en/system/files/files/sac-040-en.pdf

information sources. The objective is to influence, manipulate or trick registrants into releasing sensitive information or access to registration services. Many social engineering exploits rely on people's willingness to be helpful or fear of punishment. For example, the attacker might pretend to be a lawyer who has an urgent problem that requires access to a domain owner's registration services.

This is a popular tactic among attackers because it is often easier to exploit people than it is to find a network or software vulnerability in the registration system.

2.3.5 Protecting trademarks and well-known names

One of the risks in the registration system is the ability to register a domain name that is a trademark or well-known name. For new gTLDs, ICANN created a "sunrise" registration period, available exclusively to registered trademark holders to give them the first chance to acquire domain names matching their marks.

In order to participate in this system, registrants are required to register and validate their trademarks in the Trademark Clearinghouse (TMCH). Applications are submitted to the TMCH with information about a valid trademark from any jurisdiction in the world, including a copy of the trademark and evidence that the trademark is actively being used. Once applied for, the TMCH will verify the application for accuracy and validity[29]. Once validated, the TMCH will gain access to the sunrise registration period for new gTLDs and notifications of other parties registering potentially infringing trademarks.

The TMCH only serves as a repository of verified rights information. It does not prevent someone from registering someone else's trademarks or famous names.

Additionally, the TMCH is just one of a set of rights protection mechanisms and dispute resolutions procedures established by ICANN for its registries. The TMCH was originally set up as a tool for registries in ICANN's new gTLD programme, but since August 2020, it has been extended to the .com TLD. In addition, a range of commercial services provide brand and trademark protections for registrants.

ccTLDs, which do not have a registry agreement with ICANN, tend to use education and outreach as a tool for protecting registrants. For example, DNS.PT (.pt), the Portuguese registry operator, in cooperation with other organisations dealing with the unauthorised dissemination of copyright-protected content, has developed and hosts a portal website that provides fast and easy access to websites that offer digital content that respects the intellectual property rights of authors and creators[30].

In the Swiss registry, the registration of a .ch domain name does not require verification of the identity of the registrant. However, if there is reason to believe that the registrant is providing false identification data, is unlawfully using the identity of a third party, or will use the requested domain name for an unlawful purpose or in an unlawful manner, the registry will not activate a domain name until the registrant's identity has been verified. If a registrant fails to identify themself correctly within a 30-day period, the domain name is cancelled.

Another registry operator, EURid, uses an a mechanism called Abuse Prevention and Early Warning System, which predicts if a domain name could potentially be used for abusive purposes. If it finds that a registered domain name could be related to abuse, it will delay its delegation to the .eu zone file. EURid then reviews these domain names and potentially asks

---

[29] See https://newgtlds.icann.org/en/about/trademark-clearinghouse/rpm-requirements-14may14-en.pdf
[30] DNS.PT also publishes a quarterly magazine dedicated exclusively to cybersecurity in order to raise awareness on online threats.

the domain name holders to confirm their registration data before deciding whether the domain name should be delegated to the .eu zone file or cancelled.

In most cases – for ccTLDs – a process of risk assessment for registrations takes place as a part of delegation. In Europe there are three primary tools for risk assessment and identifying suspicious registrations: checking registration data against a database, using machine learning or AI tools to do the checking and doing validation through a stepwise set of processes. The actual process in use depends on the country that has implemented the verification process. In almost all cases, there is a formal infringement procedure that takes place when a registration has been identified as suspicious.

2.4 GOOD PRACTICES IN THE VERIFICATION OF DOMAIN NAME OWNER IDENTITY

2.4.1 Existing good practice literature

2.4.1.1 NIS Cooperation Group

The Technical Guideline: Security measures for top-level-domain name registries from the NIS Cooperation Group provides a set of measures and good practices that are specific to TLDs[31].

The guideline provides some clear measures and good practices associated with digital identity management in the DNS registration ecosystem:

Table 2 - NIS Cooperation Group, Technical Guideline: Security measures for top-level domain registries, 2022

Domain	Objective	TLD specific security measures and good practices	Details
D1: Governance and Risk Management	S04: Security of third party dependencies	TLD-01: Security of domain registrars	In case the registration process is outsourced to one or more domain registrars and there is appropriate contractual relationship between them, the TLD should ensure that these domain registrars take appropriate security measures, to protect the registration process and the registry data: • General information security good practices, such as having an ISMS (information security management system), see for instance ISO27001 • Secure access to the domain information or portfolio by the domain owner. • Secure the provisioning system: Use per domain access controls, use a unique Extensible Provisioning Protocol (EPP) "auth" code value for each registered domain name. • Support DNSSEC (Domain Name System Security Extensions)

---

[31] NIS Cooperation Group, "Technical Guideline: Security measures for top-level-domain name registries," 2022, https://digital-strategy.ec.europa.eu/en/library/nis-cooperation-groups-technical-guideline-security-measures-top-level-domain-name-registries Note that the guideline contains 26 security measures that are specific to TLDs. The ones provided here are the ones that have identity management or authentication as part of the measures described.

D3: Security of Systems and Facilities	SO11: Access control to network and information systems	TLD-02: Multi-factor authentication domain registrants	It is important to secure the access to the domain information by the domain owner, for example by using multi-factor authentication, because the accounts of the domain owners are often targeted by attackers. This is a good practice for TLDs that offer direct registration, and, if the TLD relies on registrars, the TLD should encourage its registrars to implement multi-factor authentication.
		TLD-03: Multi-factor authentications for domain registrars	It is important that TLDs use 'strong authentication', i.e. multi-factor authentication, for providing web portals access to the Registrars. Web portals provided to the Registrars by Registries are usually used to modify Registrars contact information, to load their pre-paid account, etc.
		TLD-04: Expiration of registrars credentials	In cases where it is not feasible to enforce multi-factor authentication, it is important that Registrars credentials have a limited duration (i.e. 6 months max) and that Registries implement policies to enforce passwords strength
	SO14: Protection of security critical data	TLD-16: Offer registrar and registry locks to help registrants protect their domains better.	Especially for critical domains, for example used by operators of critical infrastructure or services, it is important to allow registrants to 'lock' their domains, to prevent unauthorized changes. TLDs should offer and promote these services and make sure they are available to domain registrants

2.4.1.2 CENTR

The Council of European National Top-Level Domain Registries (CENTR) Member Security Maturity Model allows TLD managers to benchmark the maturity level of their security management, using a self-assessment scorecard. The scorecard is not available publicly[32].

CENTR has also published statistics about what data is captured (and published through WHOIS) during the registration process for both individuals and legal entities[33]. The sample size was 19 European ccTLDs. It also includes a list of data generated during the registration process (creation date, domain status, sponsoring registrar, etc.).

One of the contributors to the maturity model is the manager of the .nl domain, SIDN[34]. SIDN has produced a more general maturity model for underlying internet standards, including the standards that provide security for the DNS[35].

2.4.1.3 ISO

ISO27001 is one of the most important information security standards in the world. Maintained by the Joint Technical Committee (JTC) 1/Standing Committee (SC) 27 at the International Organization for Standardization (ISO), it is revised in 10-year cycles with mid-term reviews. The last revision occurred in 2022. It is also a formal standard, which makes it useful for governments to refer to when complying with international trade agreements and other obligations under, for example, World Trade Organization treaties.

---

[32] See https://www.centr.org/news/news/the-centr-member-security-maturity-model-is-out.html
[33] CENTR "WHOIS | ccTLD Collection/publishing of Registration Data", 2018, https://stats.centr.org/pub_whois
[34] Stichting Internet Domeinregistratie Nederland (Netherlands Domain Registration Foundation) https://www.sidn.nl/en
[35] SIDN, "A maturity model for modern internet standards", 2021, https://www.sidn.nl/en/news-and-blogs/a-maturity-model-for-modern-internet-standards

In Europe, ISO27001 is widely used as guidance for security information frameworks, including security for TLDs. The revision may include changes in formal standards for source code audits, electronic identification requirements and data integrity protection. The revision of ISO27001 may involve specifications for data integrity protection and this may lead to new specifications for requirements for digital identity, authentication and verification.

2.4.1.4 ICANN

ICANN's Security and Stability Advisory Committee (SSAC) has published several papers regarding the security of the registration process. These documents are called SAC reports.

SAC 40[36] explicitly looks at measures to protect domain registration services against exploitation or misuse. It first examines four case studies of attacks against domain name registration accounts. It then makes seven observations about the incidents:

1. "All an attacker needs to gain control of an organization's entire domain name portfolio (and to hamper authorized access to that portfolio) is a user account and password.

2. Attackers need only guess, phish, or apply social engineering techniques on a single point of contact to gain control of a domain registration account.

3. Attackers scan domain account registration and administration portals for web application vulnerabilities (e.g., SQL [Structured Query Language] injection). A successful exploit of vulnerable application code can result in the disclosure of account credentials for many domain accounts.

4. Email is the preferred and often the only method by which some registrars attempt to notify a registrant of account activity.

5. Attackers can block delivery of email notifications to targeted registrants by altering DNS configuration information so that email notifications will not be to any recipient in the domains the attacker controls through a compromised account (e.g., registrant's identified administrative or technical contact email addresses hosted in the domain).

6. Access to and the ability to modify contact and DNS configuration information for all the domains in a registration account is commonly granted through a single user account and password.

7. Even when unauthorized modification of DNS information is discovered quickly, the process of restoring DNS information to correct for a malicious configuration can be a lengthy one that is inherent in the distributed nature of the DNS and related to time-to-live values."

In a separate guide, SAC 044[37] provides a view of the same problem from the registrant's point of view. It discusses measures to protect against domain registrar account compromise and measures to detect or prevent unauthorized change activity, including a section on domain registration locks.

Even when discovered quickly, the process of restoring DNS information to correct for a malicious configuration can be lengthy.

---

[36] "SAC 40 Measures to Protect Domain Registration Services Against Exploitation or Misues," ICANN SSAC, August 2009, https://www.icann.org/en/system/files/files/sac-040-en.pdf
[37] "SAC 44 A Registrant's Guide to Protecting Domain Name Registration Accounts," ICANN SSAC, November 2010, https://www.icann.org/en/system/files/files/sac-044-en.pdf

SAC 044 was later supplemented by SAC 074[38] on registrant protection. A large part of this newer document is the identification of a credential management lifecycle including: designing the credential, creating it, distributing it, storing it, changing it, renewing it, transferring it, recovering it and, finally, revoking or destroying it.

2.4.1.5 Domain Name Association

The Domain Name Association produced a working document in 2017 called "DNA Healthy Domains Initiative.[39] A working group for the initiative identified a total of 20 practices for registrars and registries as means of combating DNS abuse. While much of the objective was focused around reducing the number of malicious websites (and, the DNS names that support them), the working group also identified "Measures to improve credential management on their platforms and minimize the risks associated with compromised domains".

In 2020 the Domain Name Association merged with the i2Coalition[40]. Verification and authentication of domain name owners no longer appear as part of the work programme for this industry-led organization.

2.4.1.6 PCI DSS

Registrars and registries that take credit card information from users are guided by the controls specifically prescribed by the Payment Card Industry Data Security Standard (PCI DSS) Compliance Obligations. PCI DSS 47[41] provides a comprehensive baseline of relevant credential management and security measures.

The following sections of the PCI DSS specifically pertain to aspects of credential management and cover in detail aspects of password length, strength, rotation, session timeouts, incorrect login attempts, minimum necessary access, etc.:

- Requirement 8: Identify and authenticate access to system components,
- Requirement 3.2: Credential storage,
- Requirements 3.5 – 3.7: Cryptographic key management.

2.4.1.7 W3C

The World Wide Web Consortium (W3C) has a Web Authentication Working Group that develops standards for defining an application programming interface, as well as signature and attestation formats that provide web application (including registration systems) with an asymmetric cryptography-based foundation for authentication of users. W3C's main goals are eliminating the use of shared secrets (i.e. passwords), as authentication credentials, facilitating MFA support and facilitating hardware-based key storage while respecting the same origin policy.

W3C's specification titled "Web Authentication: an API for accessing public key credentials"[42] is an example of a standard intended to help application designers (for instance those building user authentication tools for registration systems) build strong, attested, scoped public key credentials for applications on the web. It allows servers to integrate with the strong authenticators now built into devices, such as Windows Hello or Apple's Touch ID. Instead of a password, a private-public keypair (known as a credential) is created for a website. The private key is stored securely on the user's device; a public key and randomly generated credential ID

---

[38] "SAC074 SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle," ICANN SSAC, November 2015, https://www.icann.org/en/system/files/files/sac-074-en.pdf
[39] "DNA Healthy Domains Initiative," Domain Name Association, https://domainnamewire.com/wp-content/Health-domains.pdf
[40] See https://i2coalition.com/
[41] https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf
[42] Hodges, J., Jones, J. C., Jones, M. B., Kumar, A. and Lundberg, E. (eds), "Web Authentication: An API for accessing public key credentials level 2", 2021, https://www.w3.org/TR/webauthn-2/#sctn-intro

are sent to the server for storage. The server can then use that public key to prove the user's identity. Some registrars have already implemented WebAuthn for MFA.

2.4.2 Good security practices in verification of domain name owner identity

2.4.2.1 Two-factor authentication for registration account establishment

Discussed in further detail in Section 3.2.2 below, two-factor authentication (2FA) allows the registrar to supplement the username / password credential system by adding a second factor. The second factor can be added to the registration account setup via a third party, and consumers are used to this approach. Common 2FA approaches include requiring following a link in an email message (often tied to the username / password credential), returning a code in a text message, scanning a QR code or using a hardware token.

2FA is especially useful in protecting against brute force, automated and dictionary attacks against accounts that have already been established by registrants.

2FA also protects against bulk account creation attacks against the registrar by forcing the attacker to respond to the request for the second factor on each attempt to create an account. This provides one layer of protection against DoS attacks against the registration account creation system.

2FA has become relatively economical to implement, with custom-built open source libraries available for registration account systems.

Good practice 1 - Two-factor authentication for establishment of registration account
Objective
Improve verification of potential domain name registrants
Risk addressed
Supplement username / password credential security by avoiding brute force, dictionary and other attacks. Avoid DDoS attacks on the registration account provisioning

2.4.2.2 Using national eID, where available

For several countries in Europe, a system of national digital identities is in place. In some cases, that identity is a natural, verified one that meets the needs of the registration ecosystem and also addresses requirements in NIS2. In Estonia, local registrants use national eIDs to carry out registration at the ccTLD. In Denmark, verification of the registrant using a national eID is written into the law.

Use of a national eID is relatively straightforward in the context of national registrations, but becomes more difficult in cases where the registrations are cross-border. Solving this problem has been a project of RegeID, which intends to study and implement the opening up of registrant services provided by ccTLD registries in four European countries to the eIDAS

infrastructure.[43] This should provide a working example of how to solve the cross-border problem for the use of national eIDs in the registration ecosystem[44].

eIDAS and national ID hold significant promise for verified accuracy of registrant contact information. However, they are not yet in wide deployment in the registration ecosystem. If promoted and used where available, they would provide a firm foundation for the collection and verification of domain name owner information.

Good practice 2 - Where available, use of national eIDs as account credentials

Objective

Take advantage of existing national approaches to identifying citizens and consumers

Risk addressed

Improve domain name owner verification by using established, national eIDs. Address domain name hijacking and risks associated with attacks on credentials by using nationally verified identities

---

Case Study – ".DK", Denmark and registrations

In the late 2010's there was an increase in incidents where a .dk domain name had been used as a platform for intellectual property rights violations or abuse. The abuse involved online stores that looked normal but actually were selling counterfeit goods. The .dk registry decided that, to address the problem, it would improve the verification of the people and organizations registering in .dk[45].

For Danish customers, the registry required that registrants have a NemID card. Every Danish citizen has a national ID number. Everyone in Denmark who is over the age of 15 years and has a national ID is eligible to get a NemID card. A NemID user receives a card containing a chip that stores pairs of numbers. After logging in with a username and password, NemID users are prompted to enter a key corresponding to a number as part of NemID's two-factor authentication scheme. These private keys are for one time use only. After all of them are used, the user must get new private keys, which are generally sent to the user by post when the previous set is about to run out.

For foreign customers, the registry now does a risk assessment based on a number of different parameters. If the risk score is higher than a certain threshold, the registrant must take additional steps to document their identity. Three thresholds are in play.

- When no risk is found the domain name becomes immediately active in the .dk zone.
- In cases where there is low risk, the domain name is added to the .dk zone, but customers must document their identity in 30 days. If the registrant does not document their identity, the domain name is removed from the zone.

For foreign customers, the .dk registry operator now does a risk assessment based on a number of different parameters.

---

[43] The Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) is an attempt to create a predictable regulatory environment. The eIDAS Regulation is intended to help business, citizens and public authorities carry out secure and seamless electronic interactions. See https://digital-strategy.ec.europa.eu/en/library/publication-regulation-electronic-identification-and-trust-services-electronic-transactions
[44] Estonia has an example of this at https://registrant.internet.ee which is a registrant portal for the .ee ccTLD.
[45] Finn Petersen, "Danish Regulation on WHOIS and the effect on DNS abuse", Danish Business Authority, June 2022, PowerPoint presentation.

- The last threshold makes registrants document their identity before the domain name is placed in the zone. If the customer does not provide the required documentation, the domain name is deleted.

The impact on abuse levels in the .dk zone was dramatic. It is a case in which the public policy of the ccTLD affected the way that the registry operator and registrant carried out accuracy and identity checks.

2.4.2.3 Verifying identity through bank account and PCI DSS data

All registrars and resellers that accept credit cards for payment of registration fees can collect information from registrants that is consistent with the PCI DSS. The PCI DSS is a global standard that provides a baseline of technical and operational requirements designed to protect account data in payment systems. The current version[46] includes expanded MFA requirements in the payment process, updated password requirements and targeted risk analysis for payment processors. Specific to the registration system are enhanced validation methods and procedures.

Using the PCI DSS provides guidance on what information a registrar or reseller needs to collect in order to complete a registration payment. As part of the verification and approval of the payment process, the PCI DSS provides transactional security but also provides verification of the data provided by the registrant. The PCI DSS gives the registrar or reseller additional information to verify the data provided by the registrant and, in some cases, can help the registrar identify problematic domain registrations.

Registrars and resellers regularly use the PCI DSS to authorize credit card data. This good practice suggests that an additional step be added to use the PCI DSS system to help verify domain name owner information.

Good practice 3 - Verification of registrants' identity through bank account and PCI DSS data
Objective
Use existing payment verification tools to assist in verifying the identity of domain name owners
Risk addressed
Avoid fake registration account information by requiring verification through payment channels

2.4.2.4 Using third-party verification

Challenging attackers for supplemental identity information can make it much harder to create or use fraudulent accounts. Many registrars and resellers do not have the resources to implement identity challenges for their own system and registration flow. As a supplement to that registration flow, third parties can be used to challenge a registrant for additional identity

---

[46] See https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

information and then assess whether or not that information has anomalies that might indicate abusive or inaccurate information.

Third-party identity assessment can be based on a large variety of documentation including:

- government ID;
- driving licence;
- passport;
- credit card;
- utility bill;
- company ID;
- business card.

This gives the registrar a mechanism to include – either in the account setup or, more probably, in the registration or transfer of a domain – that provides additional tools to verify the accuracy of the contact information provided by the registrant.

Good practice 4 - Use of third-party verification, as an additional assurance layer
Objective
Take advantage of third-party verification services with the goal of improving the verification of identity of domain name owners
Risk addressed
Avoid fake registration account information by supplementing other sources of verification through third-party services. Prevent account takeovers

Case Study – Ultimate beneficial owners (UBO) registry

In Belgium, a process is in place for ensuring that the identity of the registrant is valid. This process consists of direct validation and a more indirect method.

Direct identification uses a variety of tools to validate the identity of the registrant. The first is the ultimate beneficial owners (UBO) register, a database of persons who ultimately benefit from or have a financial interest in a business or organization. An example would be an individual who owns more than a 25% share in a private company or has a similar share in a partnership. The register is a consequence of European regulations intended to prevent abuse of financial systems. Every EU Member State is required to keep a UBO register – a requirement that has been in place since September of 2020. It would seem that the register would be a consistent way to identify the legitimacy of registrants, but UBO registers are implemented differently implementations in different Member States.

Figure 2 - Current State of UBO Registers in EU 2022 (Source: Transparent Data)
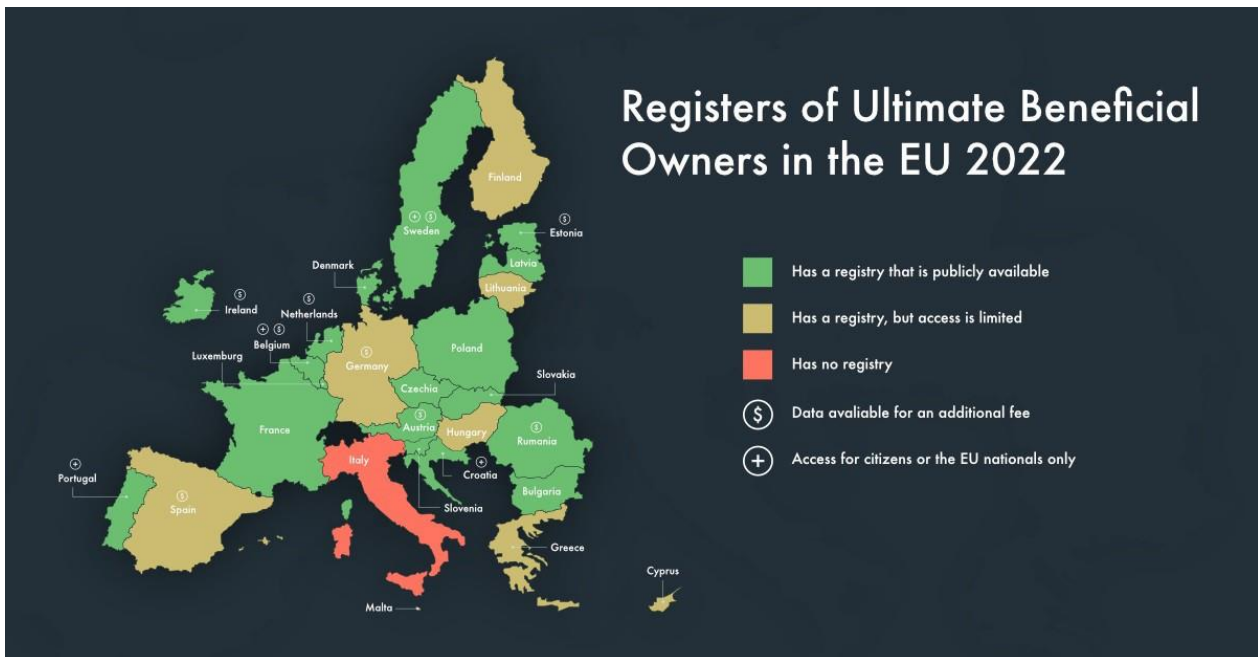
Another, formal approach to direct validation of identity is to use copies of other documents such as legal instruments or corporate documents. If there is a question about the validity of the registration, these documents can be referred to to help the registry operator assess the identification.

Sometimes the person doing the registration is not in the UBO register or mentioned in corporate documents. In these cases, more indirect forms or validation can be used to assess the registration. For example, the employee's credentials can be checked to see if they are truly a part of the organization that attempted the registration. Since many enterprises provide credentials for their employees, it is possible to perform some sort of evaluation of credentials for nearly everyone who carries out a registration on behalf of an enterprise.

2.4.2.5 Offering push notifications to registrants

Once a domain name registration account has been created, it is important for the account holder (the registrant) to be aware of any changes that take place in the contact or configuration information. Domain name owners seldom log into their accounts once a domain name has been established so they have no effective way to know if information has been changed. Domain name hijacking, for example, (see potential attack vectors, in Section 2.3.4), happens when an account is compromised and configuration data for the domain name are changed by unauthorized parties.

To address this risk, the registrar can offer push notifications to the domain name owner to indicate when a change has been made to the account. This proactively gives the registrant information about the management of their account. In the event that the registrant did not authorize the change, the process of remediation can start far earlier than if the registrant has to wait for evidence to appear on the web or by email.

Not all registrants would want push notifications, so it should be a customer choice to enable the feature. If enabled, it could be implemented through email notifications, text messages, in-app notifications or other push techniques. Like 2FA, the cost and complexity of push

notifications have been significantly reduced recently. This system helps ensure that the data stored in the registration ecosystem remain secure from unauthorized changes.

Good practice 5 - Support for push notifications to registrants
Objective   Allow domain name owners to be notified when any change is made to the records associated with their account
Risk addressed   Avoid unauthorized changes to registration accounts that may lead to domain name hijacking and other attack vectors

2.4.2.6 Using eIDAS where possible for identification and authentication

The eIDAS ecosystem provides digital identification, authentication and trust services. Because it is a transnational identity system, it can solve the problems of unequal deployment of individual member state validation systems (for instance, those in ccTLDs). The idea is to supply digital signatures and certificates that provide the same legal standing as paper transactions.

The system consists of four main components:

- a basic digital signature that contains unique information to identify its signatory, such as the name, birth date and address,

- a qualified electronic signature, which is created by a qualified signature creation device,

- a trust service that is responsible for verifying the information and data submitted by the owner of a digital signature,

- identification service providers that provide a friendly front end to the eIDAS architecture.

ID and trust services will allow registries and registrars to leverage initial registration validation processes such as 'know your customer'. 'Know your customer' is the process of identifying and verifying the identity of registrants. It can be used by registrars and registries to assess the true identity of a potential registrant and limit the number of suspicious or infringing registrations. Thanks to tools in the eIDAS ecosystem, such as notified eID, it is a process that can be conducted almost entirely online. This makes it possible for registrars and registries to more effectively establish identity at the initial registration of a domain name.

Good practice 6 - Use of eIDAS where possible for identification and authentication

Objective

Allow domain name registrants to use eIDAS as a tool for verification of identity

Risk addressed

Provide a common, standardized approach to establishing identity. Avoid risks of
infringing, suspicious or illegal registrations by using eIDAS as a tool for identity
management and verification of identity

3. AUTHENTICATION OF DOMAIN NAME OWNERS

3.1 STAKEHOLDERS AND ROLES IN AUTHENTICATION

For the purposes of this report, authentication is the process of establishing proof of identity for the purposes of managing domain name registrations. Section 2.2 on the domain name registration process, describes the business and transactional process for using a domain name registration account to manage the demographic, payment, contact, configuration and ongoing management of the information related to a domain name registration.

Thus, there are two major stakeholders in the domain name authentication process: registrant and registrar.

Figure 3 - Major stakeholders in domain name owner authentication

The relationship between the registrant and registrar is a contractual offer of services by the registrar to the registrant. The business process that makes those services work includes using an account created at initial domain name registration. The account is a service provided by the register for ongoing management of the domain name and its associated records.

As is typical in many online services, the registrant is a "consumer" in this relationship and the registrar is a "service provider". As a service provider, the registrar is responsible for providing the tools, software, databases and communications channels that allow the registrant to securely manage their domain name information.

Authentication, in this setting, is the process of proving that the digital identity of the registrant belongs to the person who should have access to the tools to manage the domain name information associated with the registration.

In some special circumstances, a registry operator also acts as a registrar (for instance in the cases of some ccTLDs). In these cases, for the purposes of authentication, the registry/registrar is in the "service provider" role. The registrant's "consumer" role remains the same.

In the case of resellers, the registrant role remains the same, but the reseller acts as the "service provider" (on behalf of, or contracted to a registrar). The security issues associated with authentication in a situation where a reseller is the provider of the domain name are the same as if the service provider were the registrar itself.

3.2 SURVEY OF AUTHENTICATION TECHNIQUES

3.2.1 Password

The oldest and most widely used authentication method is password authentication. A registrant and registrar establish a userID (often using an email address as the identifier). Then the registrant and registrar establish a corresponding alphanumeric password. The registrar often provides rules for the construction of the password (characteristics such as length and categories of characters that must be included). In some cases, the password is generated by the registrar on behalf of the registrant. In other cases, the registrant is validated with a one-time email message that then forces them to click on an embedded link and then change the password.

Passwords suffer from a variety of well-understood problems but are in wide use because the user community (registrants of domain names) is very familiar with the authentication technique. It is well known that users choose weak passwords[47] and that, even when password rules are enforced, they may be counter-productive[48]. Password managers make password management much easier for users, but take-up is spotty at best[49]. Even when users take advantage of password managers, they usually use them to store weak passwords[50]. In the cases when users do select strong, unique passwords, service providers (e.g. registrars) may instead become the weak link if they fail to follow good practices with regard to password storage. Despite these issues, a thorough review of password alternatives by Bonneau and others found that no replacement scheme comes close to supplying the benefits of passwords, and "none even retains the full set of benefits that legacy passwords already provide"[51].

Passwords are susceptible to many problems, some of which arise from decisions made by implementers[52]. For example, if the database containing the credentials contains both the userID and the unencrypted password, loss of unauthorized access to that database will compromise the entire collection of credentials. In addition, userIDs and passwords are subject to brute force and dictionary attacks. Both brute force and dictionary attacks can be automated and distributed over the network. The result is that both kinds of attacks are attacks on credentials as well as the underlying registration services themselves. Credential reuse is also a common problem with password authentication. Attackers can find databases of passwords and then take advantage of accounts that never had their passwords changed after a successful, prior attack.

Password authentication relies on a simple trust model between the registrant and the registrar. Most often the process of initial registration includes an online business process for establishing the credential.

PASSWORD STORAGE
While passwords are a common feature of the registration landscape, one of the biggest risks is in how the registrar stores the password. In the past, registrars have stored plaintext copies, stored encrypted versions along with keys and made other errors in storage. In fact, registrars shouldn't store the password at all! Instead, they should store a hash of the password.

---

[47] Florencio, D. and Herley, C., "A large-scale study of web password habits", in WWW'07: Proceedings of the international conference on the World Wide Web, ACM, 2007, pp. 657-666
[48] Florencio, D., Herley, C. and Van Oorschot, P. C., "An administrator's guide to Internet password research", Large Installation System Administration Conference (LISA), 2014, pp. 41-61
[49] Olmstead, K. and Smith, A., "What the public knows about cybersecurity," Pew Research Center, 2017, https://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/
[50] Pearman, S., Zhang, S. A., Bauer, L., Christin, N. and Cranor, L.F., "Why people (don't) use password managers effectively," in Proceedings of the Fifteenth Symposium on Usable Privacy and Security, 2019, pp. 319-338
[51] Bonneau, J., Herley, C., Van Oorschot, P. C. and Stajano, F., "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes", IEEE Symposium on Security and Privacy, 2012, pp. 553-567
[52] 81% of data breaches involve stolen or weak credentials. 73% of passwords are duplicates and at risk for credential stuffing. 17% of passwords ae the string "123456." "Security Built To Work Outside the Perimeter," Okta, https://www.okta.com/sites/default/files/pdf/SecurityOutsidePerimeterFINAL_WEB.pdf

Figure 4 - Advantages and disadvantages of passwords

AUTHENTICATION TYPE
PASSWORD

ADVANTAGES

- Relatively low cost to implement
- Low barrier for user adoption

DISADVANTAGES

- Very basic and relativley insecure authentication type
- Source of risks to both registrant and registrar
- Susceptible to DoS attack, dictionary attack and other well-known attacks
- Requires supplementary password recovery systems
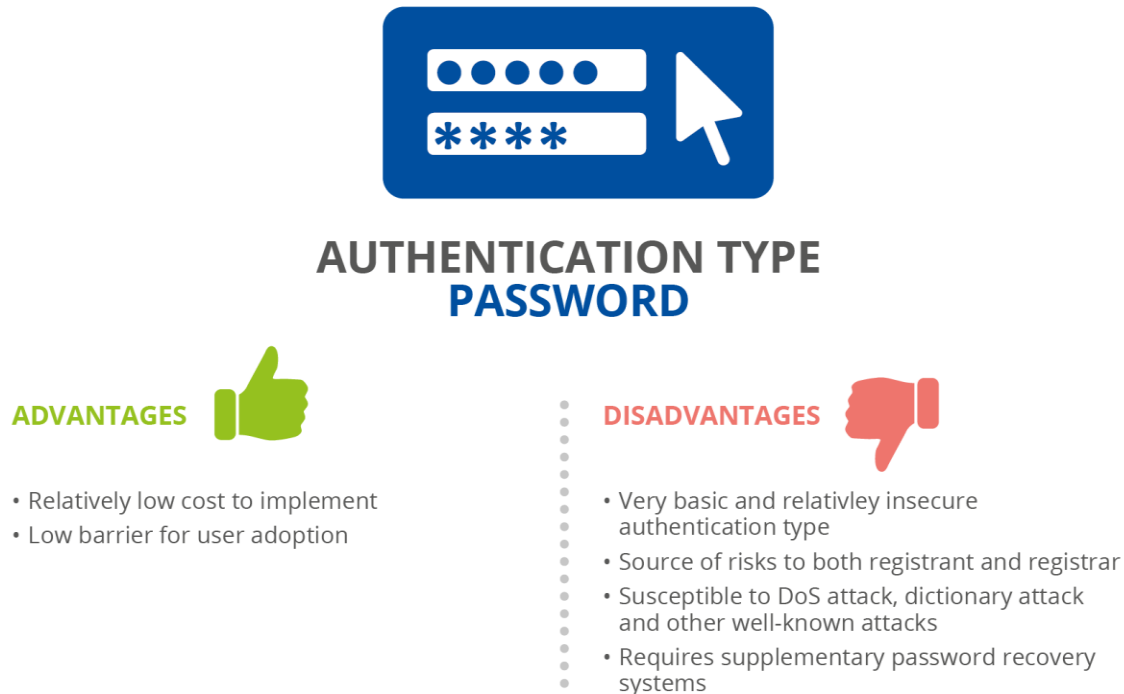
3.2.2 2FA

There is a variety of MFA techniques available. These usually combine password authentication with something the registrant has, such as a physical token, phone or other device. Two-factor authentication combines "something you know" (e.g. the password) with "something you have" (e.g. the device). Around 91% of all phishing attacks target credentials.

Hardware tokens are the oldest form of two-factor authentication. Physical devices act like electronic keys, generating a time-sensitive numeric code to access a user account. This technique may also include a wireless keycard, smart card or USB stick[53].

Text message and voice-based 2FA involves receiving a text or voice message that provides a one-time code, which must then be entered to access a site or account. In the case of voice-based 2FA, the system dials a user and verbally delivers the 2FA code.

Software tokens are a very popular 2FA form, but probably inappropriate in the registrant/registrar ecosystem. This uses a software-generated, time-based, one-time passcode or token. A user installs a free 2FA application on their phone or desktop. During sign-in, the user enters a traditional userID/password combination and then is challenged to enter the code shown on the app[54].

Push notification is a mechanism whereby websites and apps send the user a notification when there is an authentication attempt. It is a passwordless authentication mechanism with no codes

---

[53] Consumer grade hardware tokens include models such as YubiKey, Thetis FIDO2 and Google Titan.
[54] Consumer grade 2FA software tokens include apps such as Microsoft Authenticator, Google Authenticator and Authy.

to enter and no additional interaction required. The user is notified of an attempt at authentication and can respond appropriately if they were not the source for the attempt.

Biometric 2FA involves combining a traditional userID/password combination with verification of identity using fingerprints, retina, facial recognition, vocal prints or other biometric features.

All of the 2FA systems have the same basic functionality. The directory services system that holds the username and password credentials has2FA functionality added to it, which might enable it to send text messages to a user's phone or retrieve a code when a user presses the button on a hardware token inserted into a USB port. In the registration ecosystem, use of 2FA requires flexibility in the choice of the second factor. It will often be impossible to insist that a registrant acquire a hardware token, for instance. In addition, implementation of biometric solutions results in complexity and cost that may make those options unavailable to registrars.

In situations where authentication is a critical business process, 2FA has become a standard good practice. For instance, the PCI DSS, which is used to secure credit and debit card transactions against data theft and fraud, requires 2FA as a fundamental prerequisite for receiving certification[55].

2FA is widely recognized as a superior authentication technology compared with userID/password credentials. However, 2FA is not without risks. For example, using text messages to confirm an authentication attempt can be a risk in several ways. First the phone itself could be compromised and an attacker may have access to messages sent to it. Another example is when an attacker has access to the primary factor (e.g. the userID/password credential) and then uses that to change the phone number where the text messages are to be sent.

Another issue with 2FA is situations in which the consumer/user/registrant wants to revert to simple userIDs/passwords. Many 2FA systems have the ability to mark a device as "trusted"[56]. This makes it possible to authenticate without having to provide the second factor. From the point of view of the registrant or consumer, this makes sense. However, from a security point of view it now means that the trusted device is a weak link tin the authentication process. Loss of the trusted device means that an attacker could have access in a situation where all they needed was the userID/credential. Most services that provide the ability to mark a device as "trusted", also have the ability to revoke that status for the chosen devices.

---

[55] Imperva, "PCI DSS Certification", https://www.imperva.com/learn/data-security/pci-dss-certification/
[56] With user experience features such as, "Remember this computer", "Trust this device" or "Don't ask again on this computer"

Figure 5 - Advantages and disadvantages of 2FA

AUTHENTICATION TYPE
TWO-FACTOR AUTHENTICATION (2FA)

ADVANTAGES

- Many available commercial solutions for a variety of typical directory services
- Relatively low barrier for user adoption
- Successful at reducing data breaches compared with passwords alone
- Can also be used to restrict access based on other factors (time of day, geographic location)
- Extremely difficult for attackers to replicate
- Usually convenient for the user
- Less reliant on network connectivity
- Updatable with new safeguards in the future

DISADVANTAGES

- User education and engagement are important for this factor
- Requires integration into the existing authentication system (userID/password)
- Increased login time/process for registrants, with possible support costs
- Certain 2FA systems remain vulnerable to man-in-the-middle attacks
- Potential loss of the second factor
- Often requires that network connectivity must be in place for authentication to work

3.2.3 Multifactor authentication

Expanding further on two-factor authentication, multifactor authentication is a broader term that refers to multiple factors of authentication from independent categories of credentials to identify a user's identity. Like 2FA, multifactor authentication is an attempt to provide a layered defence to attacks on single credential categories. The idea is that, if one category of credential is compromised, the other categories will represent barriers to an attack on the authentication system being successful. Each additional factor is intended to increase the assurance that the person who is attempting to authenticate is truly who they say they are.

One important development for MFA is the emergence of adaptive MFA. This approach applies knowledge, business rules or policies to user-based factors, such as device or location. For example, a corporate VPN knows that it is OK for a user to sign on from home because it sees the user's location and can determine the risk of misuse or compromise. But an employee who accesses the VPN from a coffee shop will trigger the system and be required to enter MFA credentials. Adding information beyond simple credential categories can have the effect of increasing consumer adoption.

An example in the registrant/registrar ecosystem might involve including IP address origin information in the authentication process. If a registrar for a ccTLD sees an authorization attempt from an address that comes from the same country as the ccTLD serves, they might

choose not to put the attempted authorization through the process of providing the second factor. Authorization attempts from outside the country would be treated at higher risk and be forced to go through an extended authorization process[57].

Figure 6 - Advantages and disadvantages of Multifactor Authentication

AUTHENTICATION TYPE
MULTIFACTOR AUTHENTICATION

ADVANTAGES 👍

- Expands on 2FA to provide a greater level of authentication security
- Has potential to add metadata (e.g. location information) to the authentication

DISADVANTAGES 👎

- Potentially higher cost to implement
- Users (registrants) are generally unfamiliar with MFA approaches
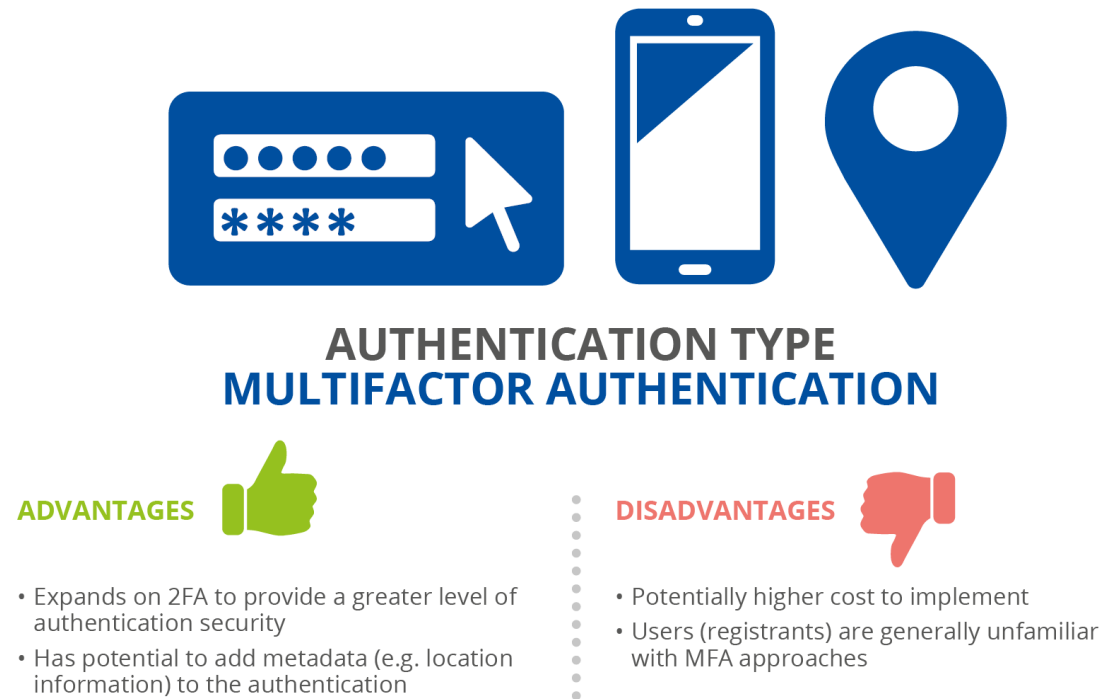
3.2.4 Social authentication

Social login, or social authentication, uses information from large global websites and social networks to facilitate logins for third-party applications and platforms. The idea is to simplify the sign-in and registration experience and provide a convenient alternative to mandatory account creation. For customers, social logins make it possible to avoid having to amass a large number of user accounts and may reduce the potential for credential stuffing. It also allows users to avoid cumbersome registration procedures to set up new accounts. For developers and applications, social authentication means either not having to build an authentication system from scratch or being able to combine data from the social network with local data for more effective user customization.

Social login is a relatively simple process that includes the following steps.

- The user enters an app or website and is given the option of selecting their chosen social network. This usually takes the form of a social login button or "Sign in with [social platform]" links. In many cases, the user is also given the option to log in with credentials specific to the app or website.

---

[57] Verisign has a patent for "Shared registration multi-factor authentication tokens". From the patent description: "A system and method for more efficiently establishing a chain of trust from a registrant to a registry. A registrant credential is associated with a Shared Registration command and is sent by a registrar to a registry. Upon successful validation, a token is generated and bound to a registrant identifier. The token is included along with the registrant identifier in subsequent discrete Shared Registration commands submitted to the registry operator on behalf of the registrant. The registrant thus needs to submit its credential only once for changes that require several discrete commands", US Patent US8769655B2, https://patentimages.storage.googleapis.com/0c/c2/d0/55a4f534c408d8/US8769655.pdf

- The social network provider receives a login request and proceeds to authenticate the user based on credentials from the social network. At this stage, users need to accept the access permissions and rules for the exchange of information between the app/website and the social network.

- The user will then get access to the site or app once the social provider has confirmed their identity.

The protocol called OAuth 2.0 is used to exchange authentication and access permissions across networks. OAuth 2.0 is not a login protocol. OpenID Connect provides the authentication needed to facility third-party logins. There are a variety of commercial providers for social authentication, but Google and Facebook currently dominate the marketplace.

For example, Google Sign-In allows users to access other websites with their Google accounts. Users can customize the information they share during authorization, but Google's social login solution currently doesn't allow for subsequent alterations without disconnecting and re-authenticating it with each third-party website[58].

Facebook Login provides a balance of convenience and privacy. While organizations using Facebook Login ultimately decide what information they request from users, Facebook's review process requires that developers provide users with a large number of permission customizations. With these permissions, users can control the degree to which they share various types of information with third-party organizations[59].

Does social authentication have a role in the registrant/registrar ecosystem? A survey of registrars serving European registrants identifies no registrar that uses social authentication as a means to authenticate domain name owners. One reason may be liability. By using a third-party authentication system, the registrar may be unable to control or influence what personal information is collected by the authenticating network. This would potentially put the registrar in violation of the GDPR. Another potential reason is that registrars have to collect a body of information that might not be available from a social authenticator. A registrar has specific requirements for the collection and publishing of accurate information (for instance, through WHOIS). The social authentication organization might not have the same requirements for accuracy or might have limitations on what data they can publish.

---

[58] It is worth noting that GoDaddy has a US patent on "Using social domains to manage a domain name registrant's social websites". From the patent description: "Methods of the present invention allow for managing multiple social websites. An exemplary method may comprise the steps of registering a domain name to a Registrant, generating a Social Domain (that corresponds to a social website) by concatenating at least one subdomain to the Registrant's domain name, mapping the Social Domain to a URL for the Registrant's social website webpage, entering the Social Domain in a browser, and displaying the Registrant's social website webpage", (US7698426B2
https://patentimages.storage.googleapis.com/f0/e4/28/7d95c88032607e/US7698426.pdf)
[59] https://developers.facebook.com/products/facebook-login/

Figure 7 - Advantages and disadvantages of social authentication

AUTHENTICATION TYPE
SOCIAL AUTHENTICATION

ADVANTAGES

- Takes advantage of well-established and secure authentication services
- It does not require to build an authentication service from scratch
- Global deployment is simple

DISADVANTAGES

- OAuth 2.0 is difficult to implement without experience
- Depends on a third party for implementation and ongoing operation

3.2.5 Alternative authentication techniques

A small number of registrars in Europe allow registrants of significant domain name portfolios the ability to use a token or smart card as a way to secure their domain name management accounts. The ability to do this, and the details for supporting it, are often under a non-disclosure agreement between the registrar and the registrant.

In addition, there are cases where individual national ID numbers are being used to identify the registrant. While national ID is a matter for member states, it appears that there is active work to bridge incompatible national ID systems where registrants in one country want to be able to register in another country that also support national IDs. So far, this is only applicable to ccTLDs that act as their own registrar/registry.

3.3 KEY RISKS IN THE PROCESS OF AUTHENTICATION OF DOMAIN NAME OWNERS

3.3.1 Unauthorized access to domain registration account

One of the key risks in the authentication process is unauthorized access to a domain registration account. The domain name registration management tools provided by registrars are subject to a variety of attacks regardless of what authentication techniques are in place. We have previously seen that credentials can be obtained fraudulently in a variety of online and offline ways. Once the registrar management account is compromised, there are significant risks to registrants, the data held in the DNS, and the function of the DNS.

- **Malicious alteration of DNS configuration**. Some of the most famous attacks on the DNS have come from compromised accounts that allowed an attacker to use the account to make changes to DNS configurations. One example is altering the configuration so that resolution of the DNS name results in A records or AAAA records

(IPv4 and IPv6 addresses, respectively) that point to destinations different from the registrants intended servers. These configuration changes can leave the registrant without Internet, email or other services and also allow the attacker to redirect services to their own services (with the consequences of malicious activity).

- **Unintentional alteration of DNS configuration**. Administrative or user error can result in risks that are similar to malicious alteration of DNS configuration. ICANN's SSAC provides an example of this in SAC 044: "Consider a circumstance where a typographical error by an authorized party sets the IP address of one of several DNS name servers for a domain name to an IP address that is not from the IP numbering space allocated to the organization. All but the incorrectly configured name servers will resolve domain names as expected. If the organization is high profile and constantly targeted, an attacker could note the addressing anomaly and attempt to gain control of the host at the exploitable address. If successful in gaining control of this address, the attacker could operate a name server for the domain name and populate the zone data for that domain with malicious DNS records"[60].

- **Malicious alteration of registration contact information.** This includes the unauthorized transfer or control of the registration of a domain name – away from the rightful registrant (domain name hijacking). It would also be possible to modify the email and postal contacts for the registration so that registry/registrar notices point to an incorrect or invalid address. Once the contact information has been hijacked it is also possible for the attacker to simply delete the domain name or influence the administrative aspects of the domain name such as renewal options or domain name locks.

- **Deletion of the registration account.** This includes the attacker simply ending the relationship between the registration account and the registrar. Consequently, this could mean the deletion or suspension of the domain name or its unintended transfer to another entity or person.

3.3.2 Failure to renew a domain name registration

- **Renewal lapse.** Unauthorized access to a registration management account may lead to the rightful registrant being unable to renew a domain name at its expiry. A renewal lapse also allows other entities or persons to register the domain name after the expiration of contractually mandated grace periods. The activities of the attacker might lead to the malicious registration of the domain name, which could be contrary to the legitimate interests of the rightful domain name owner. Worse, it is possible that the rightful registrant could completely lose access to the original domain name with implications for the costs of using a new domain name or pursuing a dispute resolution process to regain control of the domain name.

3.3.3 Non-renewal of domains associated with supporting infrastructure

- **Infrastructure renewal lapse.** The Internet landscape is saturated with dependencies between organizations to provides services, applications and information. Just as in Section 3.3.1 above, when domain names are used to resolve addresses for IP addresses, it sets up a dependency on the registrations for the infrastructure that supports those resolutions remaining in place. For example, if a company registered as company1.example is using the DNS server registered in company2.example, it is essential for the first organization that the registration in company2.example remains in-place and operational. In particular, malicious or accidental non-renewal of the domain names for the *company2.example* infrastructure is a risk that includes not just cessation of company1 services and applications, but also redirection to other servers, phishing attacks, email interception and publication of harmful or restricted information.

---

[60] ICANN SSAC, "A registrant's guide to protecting domain name registration accounts", 2010, https://www.icann.org/en/system/files/files/sac-044-en.pdf

3.4 GOOD PRACTICES IN AUTHENTICATION FOR DOMAIN NAME OWNERS

3.4.1 Securing the registration account recovery process

Insecure account recovery processes can be exploited to bypass the authentication process. Just as the establishment of the account should be protected by 2FA, so too should the account recovery process. This limits the ability of an attacker to make automated attacks on accounts through tools such as a password recovery system. If the credential recovery system uses one-time reset tokens, those tokens should be cryptographically secure random values and sent to the registrant using only secure transport (for instance, https).

If reset tokens are used as part of the account recovery system, those tokens should be invalidated after first use and have short time-to-live values (expiring in minutes and not hours). The reset tokens should also be protected so they cannot be used in a cross-site request forgery attack, in which an attacker uses the tokens to submit requests to the registration system as if they were a logged-in registrant.

Good practice 7 - Hardening of the registration account recovery process

Objective

Ensure that credential recovery systems do not become a vector for attack

Risk addressed

Avoid attacks on registration information through attempts to recover credentials (e.g. passwords). Address DoS attacks on the registration system through password recovery and other registration account support tools

3.4.2 Securing the registration management sessions

Registration management sessions are those which allow an authenticated registrant to create and manage the information held on their behalf by the registrar or reseller. Protecting those session is essential to avoid having malicious users bypass the authentication process or impersonate legitimate registrants.

When the registration management session is implemented as a web-based session between registrant and registrar, some fundamental protections can be put in place to protect the session form external abuse.

- Cryptographically secure random values should be used for session cookies

- Sessions should be managed on the server side rather than the client side.

- Cookie security attributes should be implemented, including:

  o Secure;
  o HttpOnly;
  o SameSite;
  o Domain;

     o PathExpire;

     o MaxAge.

- Session tokens should be new each time the registrant logs into the registration system and destroyed upon exit or logout.

- Idle sessions should be timed out.

<table>
<tr><td>Good practice 8 - Hardening of the registration management sessions</td></tr>
<tr><td>Objective

Protect the registration management sessions from external attack</td></tr>
<tr><td>Risk addressed

Prevent attacks on registration data by protecting the sessions between registrants and registrar/reseller management services. Ensure that sessions are established in which attackers cannot impersonate authenticated registrants</td></tr>
</table>

3.4.3 Implementation of rate-limiting for authentication attempts

Rate limiting is an essential ingredient in the protection against automated, brute force attacks. The simplest rate limiter is one that counts failed authentication attempts and blocks a user from continuing to execute attempts to access the registration management system.

Another example of rate limiting is the use of CAPTCHAs. While many users find it annoying to solve CAPTCHAs, they can be implemented in coordination with other rate-limiting approaches to avoid brute force attacks. For instance, some registrars use CAPTCHAs only in situations where a user (or, IP address) is the source of authentication requests that violate rate-limiting rules.

Good practice 9 - Implementation of rate-limiting for authentication
Objective
Protect the registration management sessions from DoS attacks based on automated authentication exploits
Risk addressed
Prevent DoS attacks based on automated, brute force attempts to authenticate

3.4.4 Hardening of password-based authentication, in cases where 2FA is not in place

Section 3.2.1 discusses the problems associated with password credentials. Registration management systems that are protected only by usernames and password share all the vulnerabilities of other password-based credential schemes. Good Practice 1 of this report suggests implementing 2FA for registration management systems, but there are clear cases in which either this is difficult to implement or the transition to 2FA is difficult.

In these cases, passwords should have strong entropy. Enforcing strong entropy can be done through a variety of password strength checkers[61], many of which are open source. The use of known passwords should be either discouraged or disallowed. Once again, public password lists are available for checking for known passwords[62] and services are available to scan passwords[63].

Good practice 10 - Hardening of password-based authentication, where 2FA is not in place
Objective
In cases where 2FA is not possible for the registration management system, protect password credentials from attack
Risk addressed
Prevent traditional attacks on password-based credentials

---

[61] For instance https://github.com/dropbox/zxcvbn
[62] See https://github.com/danielmiessler/SecLists/tree/master/Passwords/Common-Credentials
[63] https://haveibeenpwned.com/

4. CONCLUSION

The DNS ecosystem in Europe consists of a variety of stakeholders in several different roles. Those registering domain names can be individuals, businesses, public sector entities or other organizations. The process of registration involves a business relationship between registrants and registrars, which are accredited organizations that act as the retail channel for domain name registration.

The registration of domain names involves the registrants, the registrars, the registries and other companies and organizations that provide infrastructure to the public DNS. However, the DNS ecosystem is not limited to these organizations. Others have a stake in domain name registration including intellectual property holders, researchers, practitioners, law enforcement agencies, business intelligence organisations and brand protection companies.

This report has focused on the verification of the identity of the registrant during this business transaction, and the ongoing authentication of the registrant as the WHOIS records are maintained and as further management of the registration takes place after the initial registration. These are important because faulty WHOIS information can lead to DNS abuse and abuse of infrastructure related to the domain name and its subdomains. DNS abuse can exploit the registration process by allowing for maliciously registered domain names and domain names compromised by malicious parties who intend to carry out harmful or illegal activity.

The domain name registration ecosystem in Europe is diverse, sophisticated and innovative. Protecting the participants in that ecosystem starts with strong authentication of potential registrants. Without strong authentication, there are risks to intellectual property, the ability of legitimate law enforcement to investigate crimes, and an enterprise's identity and presence on the internet.

Recognizing that citizens and companies in Member States use both national registries (e.g. ccTLDs) and transnational registries, the guidelines and good practices for authentication reflect these differences. This report suggests good practices in the area of authentication that reflect the diversity of capacity of the Member States. It also provides information that could be used to help guide future implementation of features of NIS 2.

Ongoing management and maintenance of the information used to register a domain name is essential to maintaining the accuracy of that information. In many cases throughout Europe that maintenance is done through an online account with either the registry or the registrar. Once again, this report suggests good practices for the authentication of a user who seeks to maintain information related to a registration.

In addition to the good practices, this report has found that the technology and processes for both authentication and authorization are evolving. Two-factor authentication is becoming increasingly common for online access to accounts and consumers are accepting of the new technology. eIDAS is a potential tool for digital identity and should be closely examined for its ability to unify approaches to authentication in the registration ecosystem.

4.1.1 Summary of GOOD practices

No#	Good Practice	Objective	Risks Addressed
GP1	Two-factor authentication for establishment of registration account	Improve verification of potential domain name registrants	Supplement username / password credential security by avoiding brute force, dictionary and other attacks. Avoid DDoS attacks on the registration account provisioning
GP2	Where available, use of national eIDs as account credentials	Take advantage of existing national approaches to identifying citizens and consumers	Improve domain name owner verification by using established, national eIDs. Address domain name hijacking and risks associated with attacks on credentials by using nationally verified identities
GP3	Verification of registrants' identity through bank account and PCI DSS data	Use existing payment verification tools to assist in verifying the identity of domain name owners	Avoid bogus registration account information by requiring verification through payment channels
GP4	Use of third-party verification, as an additional assurance layer	Take advantage of third-party verification services with the goal of improving the verification of identity of domain name owners	Avoid bogus registration account information by supplementing other sources of verification through third-party services. Stop account takeovers
GP5	Support for push notifications to registrants	Allow domain name owners to be notified when any change is made to the records associated with their account	Avoid unauthorized changes to registration accounts that may lead to domain name hijacking and other attack vectors
GP6	Use of eIDAS where possible for identification and authentication	Allow domain name registrants to use eIDAS as a tool for verification of identity	Provide a common, standardized approach to establishing identity. Avoid risks of infringing, suspicious or illegal registrations by using eIDAS as a tool fo identity management and verification of identity
GP7	Hardening of the registration account recovery process	Ensure that credential recovery systems do not become a vector for attack	Avoid attacks on registration information through attempts to recover credentials (e.g. passwords). Address DoS attacks on the registration system through password recovery and other registration account support tools
GP8	Hardening of the registration management sessions	Protect the registration management sessions from external attack	Prevent attacks on registration data by protecting the sessions between registrants and registrar/reseller management services. Ensure that sessions are established in which attackers cannot impersonate authenticated registrants.
GP9	Implementation of rate-limiting for authentication	Protect the registration management sessions from DoS attacks based on automated authentication exploits	Prevent DoS attacks based on automated, brute force attempts to authenticate
GP10	Hardening of password-based authentication, where 2FA is not in place	In cases where 2FA is not possible for the registration management system, protect password credentials from attack	Prevent traditional attacks on password-based credentials

Table 1 – Good practices summary

BIBLIOGRAPHY

1. Bonneau, J., Herley, C., Van Oorschot, P. C. and Stajano, F., "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes", IEEE Symposium on Security and Privacy, 2012, pp. 553-567
2. CENTR, "WHOIS | ccTLD Collection/publishing of Registration Data", 2018, https://stats.centr.org/pub_whois
3. Coincheck, "Coincheck Customers Fall Victim to Data Breach After Domain Account Error", Baker, Paddy, 3 July 2020, https://www.coindesk.com/crypto-exchange-coincheck-victim-domain-data-breach
4. Cypress Data Defense, "6 Password Security Risks and How to Avoid Them", https://www.cypressdatadefense.com/blog/password-security-risks/
5. "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union", https://eur-lex.europa.eu/eli/dir/2016/1148/oj
6. ENISA, "ENISA Threat Landscape 2021", 2021, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
7. ENISA, "Mapping of OES Security Requirements to Specific Sectors", 2018, https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors/
8. Florencio, D. and Herley, C., "A large-scale study of web password habits", in WWW'07: Proceedings of the international conference on the World Wide Web, ACM, 2007, pp. 657-666
9. Florencio, D., Herley, C. and Van Oorschot, P. C., "An administrator's guide to Internet password research", Large Installation System Administration Conference (LISA), 2014, pp. 41-61
10. Freedom to Tinker, "No boundaries for user identities: Web trackers exploit browser login managers", Gunes Acar, Steven Englehardt, and Arvind Narayanan, https://freedom-to-tinker.com/2017/12/27/no-boundaries-for-user-identities-web-trackers-exploit-browser-login-managers/
11. Hodges, J., Jones, J. C., Jones, M. B., Kumar, A. and Lundberg, E. (eds), "Web Authentication: An API for accessing public key credentials level 2", 2021, https://www.w3.org/TR/webauthn-2/#sctn-intro
12. ICANN SAC, "SAC 40 Measures to Protect Domain Registration Services Against Exploitation or Misues", 2009, https://www.icann.org/en/system/files/files/sac-040-en.pdf
13. ICANN SAC, "SAC 44 A Registrant's Guide to Protecting Domain Name Registration Accounts", 2010, https://www.icann.org/en/system/files/files/sac-044-en.pdf
14. ICANN SAC, "SAC 74 SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle", 2015, https://www.icann.org/en/system/files/files/sac-074-en.pdf
15. Imperva, "PCI DSS Certification", https://www.imperva.com/learn/data-security/pci-dss-certification/
16. ISO/IEC, "Information technology - Security techniques - Information security controls for the energy utility industry", 2019, https://webstore.ansi.org/Standards/ISO/isoiec270192017
17. Krebs, Brian, "Webnic Registrar Blamed for Haijack of Lenovo, Google Domains", Krebs on Security, 26 February 2015, https://krebsonsecurity.com/2015/02/webnic-registrar-blamed-for-hijack-of-lenovo-google-domains/
18. NERC, "NERC (CIP) Critical Infrastructure Protection", https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
19. NIS Cooperation Group, "Technical Guideline: Security Measures for Top-Level-Domain Name Registries", 2022, https://digital-strategy.ec.europa.eu/en/library/nis-cooperation-groups-technical-guideline-security-measures-top-level-domain-name-registries
20. NIST, "Digital Identity Guidelines", Paul Grassi, Michael Garcia, James Fenton, 2017 and 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
21. NIST, "Guide to Industrial Control Systems (ICS) Security", 2015, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
22. Okta, "Security Built To Work Outside the Perimeter", https://www.okta.com/sites/default/files/pdf/SecurityOutsidePerimeterFINAL_WEB.pdf
23. OWASP, "A07:2021 – Identification and Authentication Failures," OWASP Top 10: 2021, https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/
24. Pearman, S., Zhang, S. A., Bauer, L., Christin, N. and Cranor, L.F., "Why people (don't) use password managers effectively," in Proceedings of the Fifteenth Symposium on Usable Privacy and Security, 2019, pp. 319-338

25. Pew Research Center, "What the public knows about cybersecurity", 2017,
https://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/

26. SIDN, "A Maturity Model for Modern Internet Standards", 2021, https://www.sidn.nl/en/news-and-blogs/a-maturity-model-for-modern-internet-standards

27. Telesign, "Telesign Consumer Account Security Report", 2021, https://www.telesign.com/resource/telesign-consumer-account-security-report

28. Verizon, "2021 Data Breach Investigations Report", https://www.verizon.com/business/resources/reports/dbir

ANNEX A:
GLOSSARY, DEFINITIONS
AND ACRONYMS

- **2FA** – Two-factor Authentication

- **Authentication** – Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system (NIST)

- **AuthInfo** - A code created by a registrar to help identify the domain name holder of a domain name in a generic top-level domain (gTLD) operated under contract with ICANN.

- **Authorization** – Validation that a user has access to a particular service or function.

- **ccTLD** – Country Code Top-level Domain (for instance, .fr or .dk).

- **CENTR** – The association of European National Top-level Domain Registries. A nonprofit association of country code top-level domain (ccTLD) registries in the European region. CENTR provides a forum where its members can discuss policy issues affecting ccTLD registries in their region.

- **Country code top-level domain (ccTLD)** - The class of top-level domains reserved for use by countries, territories, and geographical locations identified in the ISO 3166-1 Country Codes list. ccTLDs can base their names on the two-letter country codes defined by the ISO 3166-1 standard (e.g., .jp for Japan, .fr for France, .ke for Kenya), or they can represent a country or territory name in a script other than US-ASCII characters. Because ccTLDs are managed locally, the rules and policies for registering domain names vary across ccTLDs.

- **Digital Identity** - A digital identity is the body of information about an individual, organization or electronic device that exists online. Unique identifiers and use patterns make it possible to detect individuals or their devices.

- **GDPR** – The General Data Protection Regulation.

- **gTLD** – Generic Top-level Domain (for instance, .com or .org)

- **ICANN** – The Internet Corporation for Assigned Names and Numbers

- **Identity** – the set of physical and behavioural characteristics by which an individual is uniquely recognizable (NIST)

- **Identity proofing / Identity-based authentication** – A process that provides assurance of an entity's identity by means of an authentication mechanism that verifies the identity of the entity (NIST)

- **IETF** – The Internet Engineering Task Force

- **ISO** – The International Organization for Standardization

- **Mitigation** – Limitation of any negative consequence of a particular event. (ISO/IEC Guide 73)

- **NewID** – A software tool for generating unique identifiers

- **NIS** – The EU Directive on Security of Network and Information Systems

- **NIST** – The US National Institute of Standards and Technology

- **OAuth** – An industry-standard protocol for authorization. OAuth 2.0 focuses on providing specific authorization flows for web applications, desktop applications, mobile phones, and living room devices.

- **OWASP** – The Open Web Application Security Project. A non-profit organization attempting to improve the security of software.

- **PIN** – Personal Identification Number.

- **RAA** – The ICANN Registrar Accreditation Agreement

- **Registrant** - An individual or entity who registers a domain name. Upon registration of a domain name, a registrant enters into a contract with a registrar. The contract describes the terms under which the registrar agrees to register and maintain the requested name.

- **Registrar** - An organization through which individuals and entities (registrants) register domain names. During the registration process, a registrar verifies that the requested domain name meets registry requirements, and submits the name to the appropriate registry operator. Registrars are also responsible for collecting required information from registrants and making the information available through WHOIS. After registration, registrants can make updates to their domain name settings through their registrars.

- **Registry operator** - The organization that maintains the master database (registry) of all domain names registered in a particular top-level domain (TLD). ROs receive requests from registrars to add, delete, or modify domain names, and they make the requested changes in the registry.

- **Rights holder** - The person or entity that maintains a set of rights to a particular property. With respect to policy development regarding domain names, the term rightsholder often refers to a person, entity, or designee (such as a licensee or assignee) that holds intellectual property rights on a specific trademark.

- **Risk** – The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization (ISO/IEC PDTR 13335-1)

- **SSAC** – ICANN's Security and Stability Committee – established by Section 12.2 of ICANN's Bylaws.

- **Validation** - Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled (e.g., a trustworthy credential has been presented, or data or information has been formatted in accordance with a defined set of rules, or a specific process has demonstrated that an entity under consideration meets, in all respects, its defined attributes or requirements) (ISO 9000)

- **Verification** - The process of establishing an initial digital identity for the purposes of registering a domain name

- **W3C** – The World Wide Web Consortium.

- **WHOIS** – A database that contains information about registrations including registration contact information for registrant, admin, and technical contacts, the sponsoring registrar and creation, update, and expiration dates.

ANNEX B:
EXAMPLE OF A TYPICAL WHOIS RECORD

Domain ID: AAA-0001
Domain Name: example.eco
Created On: 03-May-2017 12:00:42 UTC
Last Updated On: 16-Apr-2017 16:26:58 UTC
Expiration Date: 03-May-2017 23:59:59 UTC
Status:OK
Registrant ID: ABC0001
Registrant Name: Big Room Inc
Registrant Street1: 332 – 237 Keefer Street
Registrant Postal Code: V6A 1X6
Registrant Country: Canada
Registrant Phone: + 1 604 682 6673
Registrant FAX: + 1 604 682 6673
Registrant Email: domains@home.eco
Admin ID: C5721
Admin Name: Domain Administrator
Admin Organization: Big Room Inc
Admin Street1: 332 – 237 Keefer Street
Admin City: Vancouver
Admin Postal Code; V6A 1X6
Admin Country: Canada
Admin Phone: + 1 604 682 6673
Admin FAX: + 1 604 682 6673
Admin Email: domains@home.eco
Tech ID : C5721
Tech Name: Domain Administrator
Tech Organization: Big Room Inc
Tech Street1: 332 – 237 Keefer Street
Tech City: Vancouver
Tech Postal Code: V6A 1X6
Tech Country: Canada
Tech Phone: + 1 604 682 6673
Tech FAX: + 1 604 682 6673
Tech Email: domains@home.eco
Billing ID: C5721
Billing Name: Hostmaster, Big Room Inc
Billing Street1: 332 – 237 Keefer Street
Billing City: Vancouver
Billing Postal Code: V6A 1X6
Billing Country: Canada
Billing Phone: + 1 604 682 6673
Billing FAX: + 1 604 682 6673

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.