The Role of ccTLD Managers in the Evolving Digital Identity Ecosystem

Michael Palage

The Role of ccTLD Managers in the Evolving Digital Identity Ecosystem

The Internet has transformed communications, commerce, information sharing, and the very manner by which human beings interact. However, the failure of "digital identity" to keep pace with changing international legal norms and technological developments represents a barrier to the security, stability, and inclusiveness of the Internet. This paper will illustrate how ccTLD managers can leverage their unique status as a trusted source within their communities to play a key role in the evolution of digital identity and create economic opportunities for all participants in the domain name industry.

Digital Identities in Use by European ccTLD Managers

Domain names have always played a role in digital identity. However, there is currently a paradigm shift involving this relationship. The earliest role that domain names played with digital identity were domain names (such as palage.com) and email addresses associated with them (such as michael@palage.com). While many people have integrated the use of their surname into a domain name, most have instead relied upon an email account service as a form of digital identity; e.g., AOL.COM, OUTLOOK.COM, and GMAIL.COM. However, this rudimentary form of digital identity has evolved, and now national governments and private companies are issuing digital identity credentials that provide a more robust, secure and authoritative source. As described below a growing number of European ccTLD managers are integrating digital identities into their business operations.

Estonia (.EE)

Estonia has one of the most comprehensive national digital identity frameworks and is at the forefront of the adoption of digital identity at a national level. This framework includes the following: ID-Card; Mobile-ID, and Smart-ID. In addition to being provided with a physical identification card that has an embedded chip that uses 2048-bit public key encryption, each Estonian is also allocated a personal @eesti.ee e-mail address. This government-issued email address is used for sending official communications to the individual as an Estonian citizen, and it can be configured to forward these emails to an alternative personal email of their choice.

Mobile-ID is a secure form of digital ID for use with smartphones and other mobile devices. Mobile-ID uses a special Mobile-ID SIM card, which the user must request from their mobile provider. It also uses an application on the user's mobile device to access secure e-services and to digitally sign documents. Smart-ID is a new digital identity solution that is not dependent upon a SIM-enabled device. Instead, the user only needs to install an application on any Wi-Fi-enabled device.

The Estonia Internet Foundation (EIF) requires verification of identity for all registrants of .EE domain names, and has integrated Estonia's national digital identity into this process by requiring all registrants to "sign the application submitted to the registrar either in handwriting in the presence of the registrar's representative or electronically using the Estonian ID card or Mobile ID" or to "sign the application submitted to the registrar electronically using an ID card of a foreign state accepted by EIF".[1] An Estonian digital identity is also used for security purposes when accessing the registry system. The EIF represents a unique public private partnership, where the EIF has leveraged the existing national digital identity framework to increase the overall security and stability of the .EE ccTLD.

Estonia's position at the forefront of digital identity has also provided insight into the diligence that must be employed as the inevitable prevalence of digital identity technology grows. In 2017, the hardware behind Estonian ID-Cards was found to be vulnerable to attacks, which could theoretically have led to identity thefts of Estonian citizens and e-residents. The Estonian government indicated that no such theft had occurred, and restricted access to Estonian ID-card public-key database to prevent illegal use. While a temporary block prevented the ID-card from being used for eServices for a short period (it could still be used for in-person iden-

[1] https://www.internet.ee/domains/ee-domain-regulation#identification-and-identity-verification-requirements

tification), these services were re-established within a few weeks.[2]

Denmark (.DK)

DIFO/DK Hostmaster's integration of digital identity into the .DK domain name registration process was driven in part by an effort to combat an increase in the abuse of intellectual property rights. To accomplish this integration, the registry required all Danish registrants to provide a NemID as part of the registration process. NemID is a service offered by Nets DanID A/S, which provides digital identities for both individuals and businesses. An individual NemID is available to all Danish citizens over the age of 15 who meet the ID requirements. However, there are two types of NemIDs for businesses: a NemID employee certificate which identifies an individual as an employee of that company authorized to act on their behalf, and a NemID business for banking to access corporate financial records online.

The NemID is a two-factor, single sign-on solution that is comprised of two components: log-in credentials (a user name and password) that the subscriber selects, and a physical Code Card that is provided to the subscriber. NemID also recently added an Android and iOS app as a second validation token, eliminating the need for users to carry the paper card with a one-time password. For non-Danish registrants that do not have a NemID, the registry provides an out-of-band review process using various algorithms to identify potential fraudulent registrations.

With the use of their NemID, users can access the registry self-service portal where they can perform a number of administrative tasks associated with their domain name, e.g., confirm requests, transfer, delete, change nameservers, make payments and change contacts for domain names, plus keep contact information up-to-date. Since the implementation of this registrant verification program, e-commerce storefronts suspected of violating intellectual property rights within the .DK zone file has effectively been reduced to zero.

Czech Republic (.CZ)

Unlike other ccTLD managers that sought to leverage existing national digital identity infrastructure into their operations, CZ.NIC implemented mojeID as a standalone service to facilitate the verification of .CZ registrants. A user subscribing to the mojeID service must validate their e-mail, phone and postal address by responding to PIN codes sent to each of these contact points. Subscribers can optionally visit a dedicated office and show their ID card to get the highest Level of Assurance (LoA).

The mojeID can be used by registrants to associate contacts stored in the registry database. However, it can also be used by subscribers for single sign-on services with participating commercial sites using OpenID 2.0, OpenID Connect and SAML protocols. This is a free service to the mojeID subscriber and also to the commercial sites incorporating the mojeID single sign-on functionality with the exception of when a site wants to receive a validation status for a subscriber. In this case the site pays a modest annual fee.

While the use of mojeID is not mandatory, a growing number of registrars are implementing the use of the digital identity platform in the name registration services that they provide. However, there are some services that registrants can access directly via the registry using their mojeID. Currently, CZ.NIC has also operated the eIDAS node of the Czech Republic since 29 September 2018. Although mojeID is not currently connected to either the official governmental eID platform or to the eIDAS node, CZ.NIC is collaborating with other ccTLD managers about potential future integration.

Bulgaria (.BG)

Register.BG had proactively integrated use of their national digital identity framework into the ccTLD operations of .BG as early as 2006, when it automated its systems to comply with the passage of then enacted "Digital Signature Law." In Bulgaria, every citizen is assigned a Bulgarian Identity card that (in addition to the card-holder's full name, sex and date of birth) also contains a unique 10-digit national identification number (EGN). There is also a corresponding equivalent digital identity for legal persons that contains a national identification number (EIC).

[2] https://www.zdnet.com/article/estonias-id-card-scrisis-how-e-states-poster-child-got-into-and-out-of-trouble/

Bulgarian registrants are required to provide an EGN or EIC at the time of registration, and this ID is stored in the registry database. These digital identities are used to pre-populate the traditional registrant data fields using the information from the digital identity and are also used for the following registry functions: user identification (to log in); contractually agreeing to terms and conditions; submitting requests for arbitration and authorizing changes to associated objects stored in the registry database, e.g., DNS, DNSSEC, contact persons. The .BG Shared Registry System uses the REGRR (Registry Registrar Registrant) protocol, an alternative to EPP, in which every exchanged message between the registry and the registrar is signed and recorded with encryption.

Germany (.DE)

To date, DENIC has not yet integrated any form of digital identity into the operation of the .DE ccTLD. However, DENIC has been very active in the development and pending deployment of ID4me, a federated digital identity solution. Today, most popular federated digital identity solutions are private in nature (e.g., Facebook, Google, LinkedIn.) and lack interoperability, which can lead to fragmentation, as each of them has to be implemented separately.

ID4me is being proposed as a technical standard that adds the elements of federation and DNS-based discovery to the underlying OpenID Connect standard, and as such defines an ecosystem of roles and players to provide digital identities based on ID4me protocol. In the ecosystem being proposed by DENIC, they would serve in the capacity of an Identity Authority (responsible for user authentication and consent management) and offer this “DENIC ID” service to Identity Agents. Those agents are then responsible for managing the relationship with the end user, and offering their customers an integrated digital identity product, which is again based on the ID4me standard and included in the DENIC ID.

One limitation with the current ID4me framework from a digital identity perspective is that the base configuration does not require verification of a user’s identity by a trusted source—it is a “self-sovereign” framework. However, it is possible to integrate a verified identification component into domain name records so that the ID4Me solution can operate as an authoritative source of identity. This integration of a digital identity service into the existing DNS, provides the ability of existing DNS providers such as registries, registrars and ISPs to bundle in identity solutions to their existing service offerings.

The Netherlands (.NL)

Currently SIDN has not integrated the authentication of registrants using digital identities into their registration process. However, SIDN has recently implemented a post registrant verification process in connection with suspected fraud cases where they will ask the registrant for verifying documentation. Specifically, in the case of businesses, the registrant has five days to provide documentation establishing their identity to prevent the name servers associated with the domain name from being removed.

SIDN has also been active in other digital identity initiatives. In 2017, they obtained a controlling interest in Connectis, one of the Netherlands’ leading suppliers of secure log-in solutions. Shortly after this acquisition, SIDN hosted a session with .NL registrars to discuss potential marketing of Connectis products. SIDN also recently entered a strategic relationship with Privacy by Design Foundation (PbDF), that creates and maintains free and open source software, including IRMA (“I Reveal my Attributes”) a “self-sovereign” federated identity platform. While the IRMA platform empowers users to control what attributes a user shares with a provider, it does not appear to use the DNS as a discovery method like the ID4me platform does. Recently SIDN and PbDF announced a partnership to improve the usage and availability of IRMA.

Norway (.NO)

Norid has incorporated the use of the national ID for the registration of .NO domain names as per the terms of its domain name policy. Specifically, Section 14.3 requires the domain name holder to be “identified through a unique ID; organization number for organizations, and national identity number (fødselsnummer) for private individuals.” This ID defines who has the legal right to use the domain name.

Unlike in Estonia where the government is the primary issuer of digital identities, Norway has taken a private sector approach, with the government approving five different privately-operated electronic IDs to log into the digital services of Norwegian public authorities. One of the most popular electronic IDs is BankID, a service offered by a consortium of banks, which to date have issued over 4 million digital identities.

The Future of Digital Identity and Domain Names

Approaches to digital identity are also adapting to the evolution of regulatory approaches to consumer privacy, such as the EU's General Data Protection Regulation, particularly in ecosystems of providers having "limited trust" with each other—such as with ccTLDs, and TLDs in general. In these ecosystems, there are significant benefits from the use of digital identity frameworks where personally identifying information is not transferred and aggregated with each provider in a traditional manner. Instead, a user's personal data and credentials are separately validated through an Identity Provider (IdP) for that transaction and are subsequently accessed as needed under an established set of rules.

Such approaches provide significant adaptability and potential for lower risks for data breach with respect to conventional "centralized" models. This in turn can enable organizations to provide greater value to consumers as well as more adeptly balancing consumer privacy and commercial drivers with other considerations (such as national security and law enforcement needs, due process and evidentiary requirements, data residency and similar requirements), which may also vary across jurisdictional borders.

To put this in context, ICANN's proposed Unified Access Model for continued access to registrant data is driven in large part by data privacy concerns under the GDPR. Historically, domain name registration services have been offered by competitors who each control access to the customer data that they collect—for competitive reasons, to prevent abuse of that data, for monetization, etc. These competitors must nevertheless collectively provide access to certain domain name registration data, such as for law enforcement, for intellectual property disputes, or other legitimate business reasons. The use of a federated digital identity system for accessing personal data associated with the domain name registrations will afford these organizations the ability to collectively reduce data protection costs and risks, greater flexibility in adapting data access to varying global requirements, and greater opportunity for innovating value-added services for their customers.

To better comply to privacy regulations and to reduce the risk from safeguarding personal data, federated digital identity frameworks are likely to evolve, where an IdP is used to separate identifying information from specific use / transactional credentials (like registrant, or third-party, access for domain name data). These transactional credentials can thus be pseudo-anonymized. That is, users can engage in a given transaction without having to share their personal data, yet their identity and other relevant information can still be obtained from the IdP if required, such as for a legal dispute or other lawful purpose. In this evolution of digital identity, IdP's will be custodians of personal data between users and the service providers with whom they transact.

IdPs can also act as a bridge that enables interoperability between various digital identity systems and pseudonymized credentials used for specific purposes, like domain name registrations. National ccTLD managers are a logical choice to act as an IdP in this scenario. In fact, as discussed above, some are already acting as Trusted Service Providers under eSignature frameworks such as eIDAS.

Conclusion

European ccTLD Managers are well positioned to play a thought leadership role in the continuing evolution of the digital identity ecosystem. However, nowhere may their contribution be more needed than the current debate within ICANN over the Expedited Policy Development Process (EPDP) on gTLD Registrant Data. While this diverse group of competing interests has made significant progress, there are other times that it seems to lack consensus on well-established business practices within the ccTLD community. For example, while the majority of European ccTLDs modify the output of Whois queries based on a natural person / legal person distinction, the EPDP has failed to reach consensus on whether this is even viable within the gTLD space.

While ICANN has focused almost exclusively on finding a GDPR compliant solution to its current Whois conundrum, it has failed to appreciate the growing number of national laws implementing more stringent data localization regulations. Some of the digital identity solutions being advanced within the ccTLD community, particularly for federated identities, hold the potential to provide a truly global, scalable solution to provide business predictability for registries and registrars, while safeguarding the data privacy of individuals in accordance with national laws.

centr

Council of European National Top-Level Domain Registries

CENTR is the association of European country code top-level domain (ccTLD) registries, such as .de for Germany or .si for Slovenia. CENTR currently counts 54 full and 9 associate members – together, they are responsible for over 80% of all registered domain names worldwide. The objectives of CENTR are to promote and participate in the development of high standards and best practices among ccTLD registries. Full membership is open to organisations, corporate bodies or individuals that operate a country code top level domain registry.

This paper is part of a series of articles covering industry research, historical data analysis and the future of technologies such as digital IDs, published over the course of 2019 to mark CENTR's 20th Anniversary. These publications do not necessarily present the views of CENTR or of the CENTR community.

CENTR wishes to thank and acknowledge the organisations which have so generously contributed to the efforts of its 20th Anniversary:

Platinum sponsor

.eu Powered by EURid

Gold sponsor

COORDINATION CENTER FOR TLD RU/РФ

denic

.ie IE Domain Registry

NASK .pl

.no

Your Public Interest Registry

.pt

SIDN

Silver sponsor

CAUCASUS ONLINE

INTERNETSTIFTELSEN

NETNOD

neustar

nic.at

SWITCH

CENTR vzw/asbl
Belliardstraat 20 (6th floor)
1040 Brussels, Belgium
Tel: +32 2 627 5550
Fax: +32 2 627 5559
secretariat@centr.org
www.centr.org

To keep up-to-date with CENTR activities and reports, follow us on Twitter, Facebook or LinkedIn