Identity and Trust beyond EV Certificates

Abstract

Since the emergence of commercial internet services many efforts have been made to facilitate trust in these. The CA/Browser Forum comprising a number of browser vendors and PKI certificate issuers represents one specific example of these efforts.

A major goal for this forum has been to promote secure end-to-end communication between websites and their users. This goal was only recently achieved by automating the issuance of website certificates. This paved the way for free certificate offerings which in turn allowed browsers to apply more negative indicators for unsecure connections.

Another major goal was to enable legal entities to document the relation between themselves and their online activities. These efforts have never come to fruition. Now major browser vendors including Apple, Google, and Mozilla have thrown the towel in the ring and effectively given up on their “Extended Validation” efforts.

While Google and Mozilla cite UX-problems as the reason for their removal of support for EV Certificates, this paper describes the many underlying misconceptions and flaws that has left the global business community without proper online identity and trust management.

Fortunately, considering the current state of technology, it is now possible to devise an automated alternative to “Extended Validation” that eliminates the oddities and provides innovation options with clear commercial incentives for online service providers as well as end users.

The paper concludes with recommendations to CA/Browser Forum members as well as TLD registries and Business registries on how to progress towards a future where businesses can document their identities, facilitate trust, and freely exhibit their services to end users.

Henrik Biering, Peercraft ApS
v0.98, 2020-05-03

Contents

1 History and status of DV, OV, and EV certificates

While efforts to secure HTTP communication in terms of HTTPS have been ongoing since the turn of the millenium, it was not until a few years ago that the use of encryption through the use of DV certificates surged to become the new normal rather than the exception [1] The development was originally triggered by the development of the ACME protocol that facilitated the provisioning of free DV certificates. This again allowed Chrome, Firefox, and other browsers to gradually step up [2, 3] the negative indicators for unencrypted connections.

Unfortunately this development does not apply to the additional identity assurance that OV and DV certificates were supposed to offer. Compared to the encryption option which is now typically an integral part of the service offered by hosting providers, the majority of smaller companies will find the acquisition of an EV Certificate both expensive, cumbersome, and without commercial incentives. And many of the ones that decide to aquire an EV certificate have problems in providing the appropriate information for the issuance [4].

Furthermore the common trust in the added value of OV and EV certificates has been troubled by the many incidents with misissued certificates due to carelessness [5] as well as ill intent [6] in addition to the possibilities for creating certificates with organization names matching the names of other wellknown corporations or simply statements as “Verified Company [US]” [7].

Many of the perceived problems with EV Certificates have been summarized in articles by security researcher Troy Hunt, the latest one declaring EV certificates “really really dead” [8] following notifications from Google and Mozilla of their intent to remove the indication of EV status and company name from the address bar of their browsers. This intent was realized in the fall of 2019.

The arguments presented in this article and the previous articles it refers to include

1. Users are not making secure choices on the basis of the presence or absense of EV indicators – if even noticing these (claim from Google and Mozilla)

2. EV indicators may be used for phishing attempts - or cause confusion in case of colliding or similar company names

3. Company name is not tied to users intended destination the same way that the domain name is (claim from Apple)

4. Issues with several root issuing CA’s. Problems with the issuance of intermediate certificates and EV certificates (as mentioned above) continue to emerge regularly.

5. Many large corporations do not use EV certificates. This makes it more difficult to convince small and midsized businesses of the stated EV benefits. Consequently, the adoption rate is too small to make it feasible for browser vendors to apply strong negative indicators for services not using EV certificates.

The sad thing is that during the last years deroute for OV and EV certificates, the major CA’s have been totally ignorant about the problems and have thus so far missed the opportunity to explore more viable identity and trust mechanisms for the future. Even in their reaction to the browsers removal of the EV indicator, they have consistently failed to discriminate between the principal need for dealing with web identity and trust and the obvious failure of the EV approach they have decided to cling on to [9].

2 The fatal flaws of OV and EV

This section will explore how the problems summarized in Section 1 are merely symptoms of several fatal flaws behind the whole OV/EV construct. Actually, many web users are concerned about trust and are willing to spend significant time investigating companies and their offerings. This is demonstrated by platforms such as Amazon where customer complaints as well as reviews by others are widely used as a means to build trust and remove bad or incompetent actors. So the failure of OV/EV certificates cannot be taken as an evidence that there is not a need for providing identity and trust, but rather that the issue has been wrongly addressed in several ways.

This is in line with the conclusions of a Google research paper [10] that initially states: "*Users must understand the identity of the website that they are visiting in order to make trust decisions*." and concludes: *"Browser identity indicators, including URLs and EV certificates, are supposed to help users identify phishing, socialengineering, and other attacks, but* ***prior lab studies and surveys suggested that older browser identity UIs are not effective security tools****."* and *"We conclude that modern browser identity indicators are not effective. To design better identity indicators,* ***we recommend that browsers consider focusing on active negative indicators, explore using prominent UI as an opportunity for user education****, and incorporate user research into the design phase"*.

While the Google paper strictly focuses on verifying the currently suggested problems with the EV certificate approach, this paper intends to address the underlying problems in order to provide clear requirements and propose a path towards radically more efficient identity and trust mechanisms that may function in an open ecosystem as opposed to walled garden market places as e.g. Amazon.

2.1 Integrity/confidentiality and identity are separate issues

The main purpose of DV certificates is to ensure integrity and confidentiality of the communication between a website and its users, thus preventing various types of third party attacks.

Contrary the main purpose of asserting the identity of a website operator is to ensure that users are communicating with a specific entity that they either ***already trust*** or ***may decide to trust***. It is not the basic identity that matters, but which additional claims that may be associated with the identity.

So generally speaking OV and EV certificates should not be regarded as "better" alternatives to DV certificates, but rather as products serving a separate additional purpose.

There are two distinctly different cases for the assertion of website identity:

A) The user is already familiar with the legal entity or brand operating the website and used to interact with it through the website. Typical examples of this would be the users bank, preferred search engine, or social network. If the user is adept at detecting spelling errors and noticing a possibly different TLD, he may be able assert directly from the visited URL or the sender email address that he is communicating with the proper entity or brand.

B) The user ends up at a previously unknown URL in his browser, e.g. as the result of a search or plainly by following a link. The user is now facing a problem of extracting the domain correctly from the URL (phishers can try to conseal this in the middle of a long URL) and decing on whether it is safe to interact further with the so far unknown website.

Under the constraints mentioned under **A)**, one could argue that DV certificates are fully sufficient, thus eliminating the need for OV and EV certificates. On the other hand, users missing ability to make risk assertions about new or alternatively spelled domain names as required in case **B)** may be a contributing factor to the shift from the open internet to proprietary platforms like Amazon, Uber, and AirBnB that offer implicit as well as explicit options for managing user risk.

In summary the attempt to bake legal entity information into the basic DV certificate offerings has caused immense confusion in the market – even among the CA's who should know better. Unfortunately this conflation with the DV certificate purpose has effectively led to a dead end for identity verification using OV and EV certificates.

2.2 Identity does not imply trustworthiness

Legal identity is not by itself an indicator of trustworthiness. Anyone in most jurisdictions can cheaply register a business entity, register one or more domains and set up plausible websites. In the physical world, however, setting up a business with offices in most populated locations usually implies a major investment of time and money. Most people will be suspicious if they see a branch of a major bank operating out of a campervan. Likewise, in addition to basic identity information website operators need to provide some evidence of appropriate business related efforts to prove themselves as safe to new potential users.

Therefore, the basic identity of a website operator merely serves as a handle to gather and exhibit additional trust related information about the operator. As company names are seldom unique even within a particular jurisdiction, OV certificates are not suited to provide such a basis for claims aggregation. Contrary, the unique business registry ID contained in EV certificates – *while useless for ordinary website users* – is a useful and unambiguous placeholder for gathering additional selfasserted and third party validated information about legal entities from various databases.

For this purpose business registries increasingly provide useful organisation information as open data, such as starting date, number of employees for which tax has been reported and/or annual accounts in XBRL format, all of which may be used constructively as part of a foundation for trust. For a user visiting a bank site authoritative information such as "financial institution, started 1948, 23847 salaried employees, " would represent a significantly better protection against phishing than showing the organizations name, location, and registry ID.

The ability to gather data directly from registries and from related databases has long been utilized by independent services such as OpenCorporates [11] created to allow journalists, NGOs and others easy access to such data. In view of the CA claims that EV certificates should provide user trust, one can only wonder why CA's and browser vendors have not been able to augment the useless identity information currently embedded in OV and EV certificates with information that would be more directly helpful for end users in their assessment of the trustworthiness of a website.

It is rather alarming and sad that some CA's [12] are still clearly promoting EV certificates using phrases as *"you need to communicate a high level of trust"* and *"it is safe to conduct transactions on your site"* when in fact the CA/Browser Forum EV-Guidelines [13] include a specific section on "Excluded Purposes" that explicitly states that EV Certificates are not intended to provide any such assurances:

EV Certificates focus only on the identity of the Subject named in the Certificate, and not on the behavior of the Subject. As such, an EV Certificate is ***not*** intended to provide any assurances, or otherwise represent or warrant:

(1) That the Subject named in the EV Certificate is actively engaged in doing business;
(2) That the Subject named in the EV Certificate complies with applicable laws;
(3) That the Subject named in the EV Certificate is trustworthy, honest, or reputable in its business dealings; or
(4) That it is "safe" to do business with the Subject named in the EV Certificate.

2.3 Trust is an individual choice – not a tradable commodity

The trust perceived by end users is an individual assessment based on the information available to the individual from trusted sources as well as on the individuals personal risk aversion and experience. If a user faces an unknown entity, they may often rely on the evaluation of friends or wellknown companies that have a history of interaction with the entity. In this respect trust is very unlike regular commodities that you can trade between parties. Hence, trying to sell ordinary end users trust to some company as if it was a commercial commodity – which has been the prevailing business proposition of the CA's – is quite ridiculous from the outset.

An overwhelming majority of browser users do not have the faintest idea about the various root and intermediary certificate authorities. And the small minority that do take an interest in finding out, are not likely to be impressed with Webtrust certifications that obviously only check for the technical and organisational control capabilities of the CA's. These certifications do not include any investigative actions to uncover various types of irregularities that may escape the formal controls to the detriment of end users. Webtrust reports generally contain statements like:

"The relative effectiveness and significance of specific controls at [CA] *and their effect on assessments of control risk for subscribers and relying party locations* ***are dependent on their interaction with the controls and other factors present at individual subscriber or relying party locations. I have performed no procedures to evaluate the controls at individual subscriber or relying party locations****.*

Because of the nature and inherent limitations of controls, ***[CA]'s ability to meet the aforementioned criteria may be affected****. For example,* ***controls may not prevent, or detect and correct error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements****. Also, the projection of any conclusions based on my findings to future periods is subject to the risk that changes may alter the validity of such conclusions.*

This report does not include any representation as to the *quality of [CA]'s services beyond those covered by the aforementioned criteria, nor the* ***suitability of any [CA]'s services for any customer intended purpose****."*

The evidence that Webtrust certifications are really lab tests, that do not cover actual business practices became clear when Google put pressure behind its "Certificate Transparency" initiative which led to the revelation of Symantecs more than 30.000 misissued certificates [14]. It is amazing and alarming that the Webtrust certifications appear to continue unaltered in view of the massive and persisting evidence of EV certificate issuance problems as referenced in section 1.

The user has no way to check the EV validation, that is more often than not performed by a CA residing in a completely different part of the world than where the user and the company in question is located. Just as registration of real estate, cars, and drivers licences is typically done by entities having awareness of local challenges, there are reasons to apply the principle of "Think Global, Act Local" and replace unnecessary remote entities with local and possibly authoritative trust anchors. CA's now claim [9] that user trust would increase if users were more informed to make proper trust decisions on the basis of the information in EV certificates and plea to work with browser companies to evolve the EV-indicators rather than deprecating them. This is a fairly dubious claim.

Lets assume that a person has doubts about whether the domain ***abnamro.nl*** really represents the major dutch bank ***ABN AMRO*** [NL 34334259]. Most users would turn to somebody they have an existing relation to. It could be either a local dutch directory or a global service provider such as:

Google: https://www.google.com/search?q=abn+amro+bank (First search result)
Facebook: https://www.facebook.com/pg/abnamro/about/ (134k+ followers)
Linkedin: https://www.linkedin.com/company/abn-amro/about/ (10.001+ employees, 26k+ on Linkedin)
Twitter: https://twitter.com/ABNAMRO (76k+ followers)

This illustrates that the web has now reached a state where many companies have succeeded in creating a complex online presence that corresponds to the efforts required to establish a trustworthy identity in terms of erecting office buildings and creating business reputation in the physical world. For the future it would be desirable to be able to capture and associate such “graph” information for businesses along with their basic authoritative identity attributes.

Contrary, if the user decides to investigate the EV certificates of websites as ***abnamro.nl*** to form an opinion of the trustworthyness of the sites, he will quickly find the following information about the trust root:

- A root CA, Quovadis Limited (BM 28474), located in Bermuda, a country pendling between the EU blacklist and graylist for countries supporting tax evasion [15]
- The root CA and several members of its management as listed on quovadisglobal.bm appear in the leaked “Paradise Papers” [16]
- A longlasting relationship with the dubious UAE company Darkmatter [6, 17]
- Vetted by Webtrust certifications that are mostly disclaimers as referenced above [18]
- While quovadisglobal.bm is obviously firmly associated with the root CA Quovadis Limited (BM 28474) (by contact info, certificate application forms, attestations and massively throughout the text of the website), it is using an EV certificate issued to a another CA business in Utah, USA (possibly a parent of BM 28474, but nevertheless misissued) [19]

If information from EV Certificate chain inspection was their only basis for assessing the identity of ABN AMRO Bank N.V. (NL34334259), customers investigating the certificate would probably instantly start looking for another bank.

Until identity certificates are signed by real authorities rather than unknown remote CA’s the most effective identity and anti-phishing mechanism on the internet will probably remain the the 1883 Paris Convention for protection of trademarks. If anyone else started offering banking services on ***abnamro.nl*** they would rapidly face a ton of lawyers and be shut down one way or another.

Also, existing customers who know the online location of ABN AMRO would gererally be much more likely to trust a TLS certificate signed by a non profit (as LetsEncrypt) supported by a slew of large wellknown organisations and an automated process than trusting a commercial CA whose business practices are aligned with the entities seeking certificates rather than with the end users. A recent comprehensive analysis of PKI Incidents [20] supports this more broadly by concluding:

> *“We found several cases where CAs designed business models that favored the issuance of digital certificates over the guidelines of the CA Forum, root management programs, and other PKI requirements. Examining PKI from the perspective of business practices, we identify a taxonomy of failures and identify systemic vulnerabilities in the governance and practices in PKI. Notorious cases include the “backdating” of digital certificates, the issuance of these for MITM attempts, the lack of verification of a requester’s identity, and the unscrupulous issuance of rogue certificates.”*

This kind of problems related to vendors seeking to sell consumers trust in a business entity is certainly not unique to the certificate issuance business. Similar flawed practices are seen in various types of directory and reputation services where vendors are paying third party services to gather reviews and scores from their customers. By necessity their business models are based on discrimination between their paying customers and non-paying businesses. The only ways to avoid bias between evaluation of service provider identity and trust within an ecosystem is to create:

a) walled gardens based on common mandatory trust frameworks (platform approach)
b) mechanisms that are essentially free to use for service providers in an open ecosystem
c) mechanisms controlled by service recipients or their agents (as opposed to service providers)

Services like LetsEncrypt is an example of b) and DANE a correponding example of c) for enabling encrypted communications between websites and clients. The purpose of this paper is to pursue equivalent type b and c) mechanisms for identity assessment of the businesses represented at websites.

2.4 Domain level identity is not sufficient

In the physical world it is well known that you have to distinguish between ***where*** (location) and ***who*** (entity) you are dealing with. Registered landowners with several leasers are seldom directly responsible for any specific actions of their leasers. When buying infected food from a vendor on a market place or making a deal with a company in an office mall, these specific entities are the primary targets for complants and lawsuits, and therefore also the ones you need to identify and probably examine more closely before dealing with them. The market place or office mall owners may provide assistance with this, but will only be liable in exceptional cases.

Illustration 1: Farmers Market, Mountain View, Copyright: SK@Flickr, Licence: CC BY-ND 2.0
(transparent market places still exist – even in Silicon Valley)

Similarly, in many cases internet domains names may be associated with a multitude of legal entities. From a customer perspective it is of secondary interest who is technically running the website, but of primary interest who they are legally interacting with, e.g. when making a purchase. In particular, to avoid confusion, there must be consistence between the self-asserted identity information presented by the entity in the main browser window and any authoritative entity information provided by the browser. Therefore, there is a need not only to associate identity with fully qualified domain names, but more broadly to individual paths under a domain or even with different page versions sharing the same path. The examples below are provided to illustrate the wide variety of cases, where the OV/EV certificate construct falls short of meeting reasonable user expectations.

Page related entities

- ***International corporations*** that have invested large amounts of money and efforts to establish local brand presence in many jurisdictions often choose to operate their localized services under different path segments of a .com domain. But they have no interest in having browsers indicating a different country/jurisdiction than the one corresponding to the localization selected by a specific customer or partner. Indeed it is a strong trust parameter in many parts of the world to clearly demonstrate that a business has a locally incorporated subsidiary.
- ***Agents*** have traditionally facilitated sales in various business areas, e.g. travel, where the risk of either the service (airline/hotel) or the agent business going bankrupt has traditionally been relatively high. Also the liability towards the consumer in such cases may depend on the arrangements between service providers and agents. A browser indicator that does not properly indicate who is the contracting entity may cause confusion and subsequent losses for either consumers or business entities.
- ***Platforms*** typically represent a further development of the agent business model. While some platforms like Amazon present a mix of own sales and third party sales, most platforms have incentives to demonstrate that they are not legally responsible for the content on the platforms and defer this to the extent possible to the service providers operating on their platform, e.g. Uber (employment laws) and Facebook (laws covering criminal acts).

End user dependent entities

- ***Globally branded corporations*** may go even further in this direction by using the same paths across several jurisdictions, while using technical attributes and/or user interaction to determine which legal entity the user is deemed to interact with. ***Google*** is a key example of this approach, where the identity to be displayed is neither determined by domain nor path:

  If I am in the EU, the URL: https://policies.google.com/terms?fg=1&hl=en
  provides the message: *"Welcome to Google! Thanks for using our products and services ("Services"). If you're based in the European Economic Area or Switzerland, unless stated otherwise in any additional terms, the* ***Services are provided by Google Ireland Limited*** *("Google"), a company incorporated and operating under the laws of Ireland (Registered Number: 368047), and located at Gordon House, Barrow Street, Dublin 4, Ireland."*. But accessed from another country (e.g. Ukraine), the message contained in the exact same URL changes to: *"Welcome to Google! Thanks for using our products and services ("Services"). The* ***Services are provided by Google LLC*** *("Google"), located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States."*

The ability to properly manage these cases that are typical for larger corporations is particularly important due to the difficulty in convincing SME's to adopt measures that are not being used by larger corporations. It also demonstrates that any efforts to provide identity as a basis for trust must reflect the actual end users location and situation rather than being fixed by some remote verifier.

2.5 Trust assertions can be complex and fast changing

The use of third party issued certificates to provide trust in different business contexts is certainly not new. It has been in use to document the various skills and virtues of craftsmen for centuries before the advent of online interaction and trade.

Illustration 2: Identity papers and certificates [Cory Doctorow - CC BY-SA 2.0]
(signed directly by the respective authorities – not by proxies)

All of these third party claims have traditionally been recorded separately and signed directly by the entity responsible for the claim, i.e. the business license was signed by the local government authority, the skilled workers certificate by the professional examination entity, and so forth. Lacking the equivalent of verifiable digital signatures, the certificates were often produced using special printing and engravement methods that made them difficult to falsify using contemporary technologies.

When digital certification technologies and needs evolved, traditional authorities were ignorant about them. This created a hurdle for the creation of trustworthy identity-based digital services in many areas. So it is not surprising that the resulting frustration in the respective markets has given rise to a number of proxy provider frameworks such as the CA/Browser Forum and the Global LEI Foundation. Unfortunately, this has resulted is trustchains that are quite irrational as already described using the ABN AMRO example in section 2.3. Furthermore the proxy frameworks with their infrequent assessments are only suited for information of extremely static nature as update and revocation handling is a non trivial problem in a rapidly changing world, and difficult to monetize in the proxy business model.

Some EU institutions are currently further escalating these proxy related problems. Rather than having claims from different authorities being signed by the individual authorities or their proxies, authorities related to the eIDAS and PSD2 implementation regulations have worked to extend the proxy role to aggregate claims from several authorities in very costly bulked claim certificates. Although this move may be attributed to the current digital illiteracy of the national financial EU institutions it is definitely a questionable and not scalable practice. A general store which may want to become a Payment Initiation Service Provider (PISP under PSD2) may also be subject to a long list of other regular examinations and certifications from a wide variety of public and institutional authorities. So trying to aggregate all such claims in a single certificate would lead to large costs and revocation risks for businesses and place the QTSP’s in a questionnable gatekeeper position.

Fortunately many other EU authorities, e.g. food safety authorities, are far ahead of the EU digital identity authorities in following high level political intents for implementing open API's in support of a realtime digital economy. This allows any user or user agent to gather authoritative claims directly from their sources and let users draw conclusions based on their own perspective and assessment of these claims.

Also it is customary for business registration authorities to start a resolution process for businesses that are failing to submit reports after due notice. In some countries this is instantaneously being reflected in the business name (e.g. "XYZ Ltd. Under forced resolution") and should thus automatically result in a revocation of an EV Certificate. Some businesses may be inspired to submit their reports and seek suspension of the resolution process within a short period of time after receiving such notifications. Nevertheless, an EV certificate should be revoked in the meantime, which means that the business would have to undergo a new CA assessment to get a new certificate. This would be avoided in an API economy where users make decisions based on realtime status and only rely on certificates as a short-time fallback mechanism for identity and trust related claims to avoid downtime, performance issues, or undesired user activity leakage.

2.6 Plain browser indicators for trust are too little too late

When persons browse the open internet or platform managed market places, it is most often not because they want to interact with a specific known business or at a specific location (domain or specific URL). Their main interest is to gather information or buy products and services safely at the best possible terms according to their own preferences.

In the early days of the internet the combination of simple user agents and primitive search engines worked out well to solve this task. There were seldomly more than 10 online suppliers of a particular type of products. A search on Altavista, Google or Yahoo would freely reveal them all and persons wanting the product or service could easily check out all of the provided search results.

Today there are 100.000's or millions of online suppliers of many specific types of products and services. But still relevant identity and trust related claims as well as user preferences are not being considered before the person has navigated his browser to the URL of the specific supplier. Thus it could easily take a person more than a year to locate the product or service representing the optimal choice. So instead users skip the full search process and simply select one of the vendors that made it to page one of the search engines result pages by paying the highest fees to the search engine.

Further, the overwhelming number of serious businesses creates immense opportunities for various types of fraudulous actors to blend in with the crowd, whether they are just SEO experts making false claims about product details or criminals phishing for user credentials and data.

This is again a major reason behind the current move of business from the open internet to confined market places for various types of products and services like Amazon, Uber, AirBnB, and Upwork. Generally these services are collecting and verifying supplier information at sign up as well as monitoring supplier performance and reputation in various ways. Subsequently this information is used to prioritize which suppliers are presented as first choices to customers. And customers appreciate the process as being both convenient and safe compared to generic internet search.

To preserve – or even regain – an open internet where persons can make optimum product and service choices, it is essential that businesses can make relevant identity and trust related claims available to facilitate preselection of vendors according to customers specific preferences. As an

example, persons needing a carpenter to build their new house, may generally prefer their browser or search engine to only display examined carpenters who can document a valid professional insurance policy. Similarly, if many businesses offer equivalent prices and terms, many persons will have a standard preference for the ones paying taxes in their own jurisdiction.

In summary: As digitization and globalization proceeds it is essential that businesses and persons become able to find and interact with each other in ways that are not only convenient, but reflect the various qualities of the businesses and their offerings versus the preferences and trust elements relevant to specific customers. Generically discoverable identities offer immense opportunities for development of todays primitive user agents into AI assisted semantic web browsers or develop a next generation more person centric and facts based e-commerce search engine. But it is all based on the ability of businesses to exhibit – in an commonly discoverable way – not only self-asserted data, but in particular verified third party claims about various aspects of their business conduct.

2.7 Costs and hazzle with insignificant value proposition

As a result of the various flaws and deficiencies mentioned in the preceeding sections the use of EV certificates has not reached a any critical mass needed to serve as a backbone for service provider identity on the internet. Instead platform providers as GAFA and similar twosided platforms have used a pallet of measures to provide their own identity and trust framework silos to steer users gently and elegantly to providers that the platform owner considers safe and have a profitable business relationship with. EV Certificates totally fail to offer such business incentives, as

- their influence as a signal late in a users journey severely limits their impact on user choice
- the provided identity is ”a dead end” not easily leading to discovery of further information

Contrary, they represent added hazzle and costs. Single domain EV certificates have a direct cost varying from a couple of hundred to around 1000 USD pr. year. Moreover, they are incompatible with the lower price tiers of popular DDOS and WAF-services such as Cloudflare, that only supports EV certificates for tiers ranging from 200 USD upwards pr. month.

In addition the issuance and maintenance of EV Certificates involve internal efforts which may represent even higher levels of cost relative to using plain ACME based certificates. In particular this is due to the required coordination efforts between tech, legal, and sales/marketing areas involved in EV certificate management. While DV certicate management (message integrity) is a tech issue, identity is a legal issue, whereas customer trust is a sales/marketing issue. So even allocating the EV costs with one of the respective departments in the organisation could be an issue.

Currently there seems to be a dialogue between some CA’s and the Global Legal Entity Identifier Foundation (GLEIF) [21] . GLEF was founded after the financial crisis in 2008 by financial authorities out of frustration with their inability to identify parties to transactions across markets, products, and regions. Based on its mandate the GLEIF with its associated LEI issuing organisations (LOU’s) has developed into an openly accessible proxy for basic business identity information from jurisdictions where business register information is still difficult to access or guarded by paywalls. In isolation LEI’s have limited value as they do not involve cryptographic mechanisms or any verifiable digital end-points enabling LEI holders to prove their identity.

Some kind of cooperation between CA’s and the GLEIF may thus prove beneficial as part of efforts to avoid the ”dead end” problem mentioned above. However, the increasing direct availability of information from business registries and the efforts such as BRIS [22] to align Business ID formats and information schemas across jurisdictions will eventually make LEI’s redundant.

3 Developing service provider identity and trust

In Sections 1 and 2 we discussed todays failed business identification practices. Several of the reasons for this failure relate to the confusing and unnecessary conflation between basic identity proofing and the establishment of secure communications between parties. So a main aim of this section is to describe a way forward for identity assessment that eliminates this conflation.

It would also be a goal to automate the basic identity assessment similarly to the free ACME certificates that are now offered by default to the customers of many major hosting providers.

Further it is important that new solutions do not stop with basic identity claims, but provide a method to relate additional identity and trust related claims to the identified entity. Entities must be able to publish such claims in a way that is conducive to attracting and retaining more customers.

Finally, such a next generation identity and trust framework must have proper transition and fallback mechanisms for support of legal entitities in digitally less developed jurisdictions.

A high level specification compiled on the basis of these various concerns is provided in Section 3.1 while possible ways to fulfil the various requirements are outlined in the subsequent sections.

3.1 Core requirements

A) **Provide** a basic mechanism for authoritative association of a legal entity with its online resources …

B) … that will allow frictionless direct validation of legal identities to effectively enable free provisioning (similarly to the ACME provisioning for DV certificates)

C) … that shifts responsibility for validation from the service provider side to user side agents and enable a reduction in validation intervals from years to days – or even realtime, if needed

D) … that will function independently from integrity/confidentiality preserving (TLS) certificates whether these are CA signed DV certificates or have their legitimacy asserted via DANE

E) … that will function whether these resources are associated with fully qualified domain names or individual webpages (URL's) on domains hosted by other legal entities

F) **Provide** a) to f) in a way that allows service providers to easily extend their basic identity claims and resources with further self-asserted and third party validated claims …

G) … for contextual aggregation and processing by search engines as well as user agents

H) … suitable for use by next generation data driven "Personal AI"-based user agents

I) **Provide** a bootstrapping mechanism that will allow resolvers or end user agents to "whitelist" generally recognized service providers

J) **Provide** a fallback/transitional mechanism to support CA or other third party validations for entities where the full functionality as described in a) to f) is not yet available or feasible

K) **Provide** commercial incentives for legitimate companies and facilitate competition for transparency and validation options among business and .tld registries as well as for other types of service providers and validation providers.

3.2 Automated baseline identity

The basic prerequisite for asserting that an online resource is controlled by a specific business entity is mutual referencing:

- **The business entity claims ownership of the domain**
- **The domain controller claims that the domain represents the business entity**
- **A verifier asserts that such mutual claims are matching**

Once such a relation between a business entity and a resource has been established, it may be used for identity verification by parties engaging with the resource end-points.

The complexity currently involved with EV validation is largely due to the CA's indirect reception of claims through alleged representatives of "applicants" who may well be imposters. Ensuring that such self asserted representatives are indeed authorized to both 1) represent a specific business entity and 2) can exercise control over a claimed domain is certainly non-trivial, in particular following the introduction of personal privacy laws such as the GDPR. Also, the non transparent process requires that the verification of the match between the mutual claims is performed by the CA when it conducts the issuance process rather than ad hoc when needed by relying parties.

In this section we will look at emerging options for eliminating the EV related complexity relating to the verification of the applicant and how this facilitates ad hoc client side verification.

1. ***The business entity claims ownership of the named resources***

In many countries national or local authorities have been registering legal entities for more than 100 years. While the internet was developed and grew the filings with these registries were still mostly paper based. Therefore, proxies like CA's were needed to ***a)*** query the business registries for lists of registered officers, ***b)*** verify the identity of these using scanned identity papers, and ***c)*** to have them confirm that a claim of ownership to a domain made by an employee of the business was indeed authoritative from the perspective of the business. This is a manual multi-step process prone to human mistakes.

By now, however, most jurisdictions have replaced the paper-based archives with digital systems and many local registries across all continents have followed government open data policies to provide open access to registry data [23]. Basic data for more than 180 million legal entities are already available via API's or as bulk downloads. For the EU, the new "Open Data Directive" [24] coming effectively into force by mid 2021 ensures that rich information about companies and company ownership will be available from all EU countries. The UK, now leaving the EU, has already made such rich company data available.

This requirement for openness also reflects the original rationale for granting limited financial liability to some types of corporations against requesting transparency regarding their operations. As a parallel effort many registries have increased their security measures, e.g. to require national eID's supporting two-factor login for owners to update business registrations.

Business registries have traditionally been listing the physical address of the companies to enable authorities, potential customers, and investors to contact or visit a company to gain information about its operations, services and financial situation. A digital endpoint in the official business records not only enables real time communication, but also eliminates the need for the current indirect process of communicating via people, whose relation to the business must be verified.

But amazingly it has taken more than 50 years of internet and 25 years of WWW before the business registries have noticed that many companies are now completely digital, maintaining physical or POB addresses for formal reasons only. Business registries are now beginning to enable the registration of online addresses (URL) as part of a company's basic official record. The first implementers were Norway (now for 161.000 companies) and Finland (125.000) followed by Denmark (90.000), New Zealand (85.000), Greece (52.000), and very recently Belgium and The Netherlands. Adding an extra field to its records is a relatively simple issue for a business registry – and completing the URL entry has been proven trivial for users: the numbers above (mostly from [25]) already represent a significant proportion of the businesses in the respective countries.

Jointly, these two developments – open registry data and the inclusion of a digital end-point – enable a business to directly make an authoritative and persistent public claim about its domain ownership, thus bypassing the laborious CA based process.

2. *The resource controller claims that the resource belongs to the business entity*

When users are interacting with a website, their legal options and their related trust may significantly depend on whether they deal with the domain/brand owner or an easily disposable and replaceable subsidiary or affiliate.

The basic method for a serious business to convey its identity to users is to register its domains in its own name / BusinessID and ensure that this is correctly reflected in the WHOIS information. This is in line with the CA/Browser Forum EV Guidelines [13] stating:

> **11.7.1.Verification Requirements**
>
> (1) For each Fully-Qualified Domain Name listed in a Certificate, other than a Domain Name with .onion in the right-most label of the Domain Name, the CA SHALL confirm that, as of the date the Certificate was issued, the Applicant (or the Applicant's Parent Company, Subsidiary Company, or Affiliate, collectively referred to as "Applicant" for the purposes of this section) either is the Domain Name Registrant or has control over the FQDN using a procedure specified in Section 3.2.2.4 of the Baseline Requirements.

In many cases, however, business entity data cannot be adequately determined from WHOIS data:

- **a)** Currently only a small number of registries, including the Finnish (.fi), Norwegian (.no) and Swedish (.se) are including the unique BusinessID's with the WHOIS information
- **b)** Entities with similar or even identitical names may be created with some business registries. Some registries allow matching names with just the legal type differing. And entities facing bankruptcy often make last minute name changes to be able to create new entities with names matching the original name of the entity facing bankruptcy
- **c)** WHOIS data from the TLD lack security (RDAP) and/or are not properly internationalized
- **d)** Some domain registries hide not only personal registrant identity, but also business registrant identity out of (mistaken) privacy concerns, or the entity itself has selected a privacy proxy although this counters the idea of ID validation
- **e)** For a number of practical reasons a domain may be registered by another entity than the one whose activities it represents
- **f)** Often a domain is intended to represent a number of different entities as previously described in Section 2.4

Building a resolver to derive the proper internationalized BusinessID from existing WHOIS information could eliminate the need for domain registrants that are controlling their own domains (possibly including some group b) and c) entities) to make any additional claims about the business controlling the domain. So this should be considered a fallback option when implementing transition mechanisms as described in section 3.4 to accelerate the adoption of OpenDiscovery.

The basic general method, however, must be for the domain controller to ensure that its BusinessID is directly and easily discoverable, which may be done in several ways, e.g.:

a) Providing the BusinessID to the domain registrar/registry (for ID supporting registries)

b) Creating a BusinessID entry in the DNS record for the domain

c) Creating a BusinessID entry under .wellknown for the domain

d) Adding the BusinessID as an HTTP response header field. This method will allow domain controllers to delegate the authority for individual pages to different business entities

Each of these methods have advantages and drawbacks, so it is envisioned that any OpenDiscovery resolver/verifier must be able to support all of them.

3. ***A verifier asserts the match of the mutual claims***

Based on simple claims by business entities and by domain controllers as described above, anyone with data access to business registries can now easily capture the data to validate if a claim by a business entity that it controls a domain or vice versa is mutually acknowledged.

Some important implications of this validation concept relative to EV certificates are:

a) users do not have to trust identity claims provided by an arbitrary service provider (i.e. “Certificate Authority”) having the business as beneficiary. Instead users can select a service provider that they trust (i.e. “user agent”) to perform identity verification for them as they engage with businesses.

b) validations can be performed whenever needed using similar “time to live” schemes as typically used for DNS entries rather than the CA validation practices with intervals of more than a year.

c) the complexity and effort required from businesses to be identified is significantly reduced

In summary, this new baseline identity validation method can be implemented by simple means to meet requirements A) through E) as stated in Section 3.1.

It suffers, however, from some of the other problems mentioned in section 2 and thus fails to meet the remaining requirements stated in Section 3.1, including:

d) options to enhance the identity information to provide a basis for proper trust decisions

e) support businesses that are controlling multiple resources (domains / URL’s)

f) means for using this information as part of users search criteria rather than post search only

Handling of these aspects will be covered in Section 3.3, while bootstrapping and fallback mechanisms to create synergies with the current EV scheme in order to increase adoption will be covered in Section 3.4.

3.3 Resolution and extensibility using OpenDiscovery

This section outlines how a simple protocol and resolver may retrieve self-asserted as well as third party validated claims about a business entity and its resources based on its internationalized BusinessID. The assumption for the resolution process as illustrated in the figure is that a user has located an online resource, e.g. by browsing to a website. The users agent has then discovered the BusinessID claimed by the resource controller using one of the methods described in Section 3.2.

The first step in the resolution process is to locate the authoritative business registry. This can be compared to resolving the TLD registry for a DNS lookup. It requires a comprehensive list of the various national business registries and agreement on the schema for the registry identifier part of the internationalized BusinessID. In the EU this has been officially determined by the introduction of the EUID as part of the aforementioned BRIS efforts [22]. Some organizations are currently developing global registry overviews that could potentially supplement the EU BRIS efforts in the remaining parts of the world. Examples of such initiatives to index business registries are GLEIF [26] and CA/Browser Forum [27], the latter initiative currently demonstrated by Digicert [28].

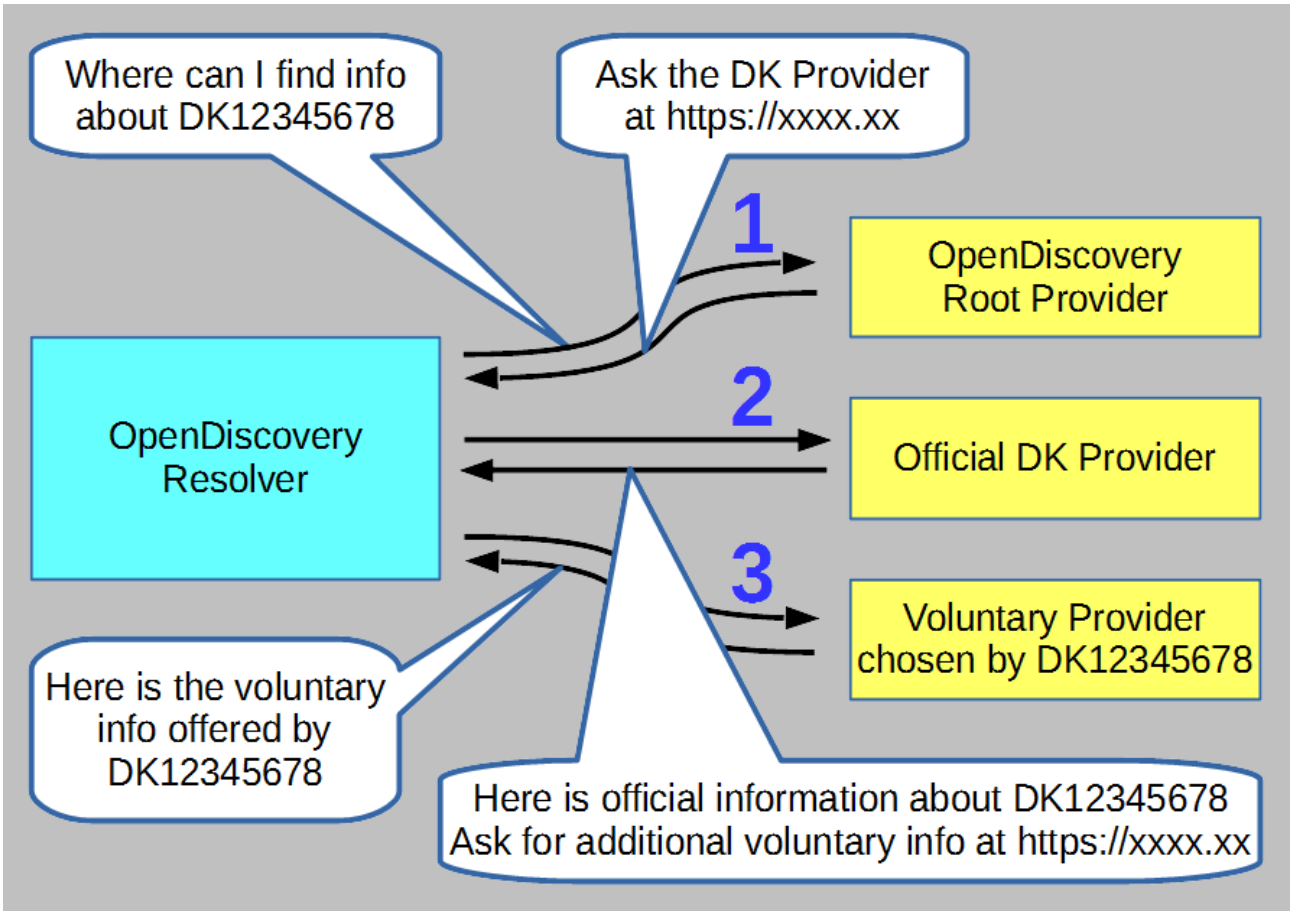

Illustration 3: Overview of the OpenDiscovery Business Information Resolver

The second step in the resolution process is to query the authoritative registry for information about the business entity. Automated realtime execution of this step requires that the registry supports (free) lookups based on the local part of the internationalized BusinessID. It also requires that the data available includes a homepage address (domain, URL). For the many SME's that have only registered a single domain, the identity of the business can be validated at this stage. And the identity profile may be enriched by any relevant additional data available from the registry, such as date of incorporation, number of employees, or financial data.

In the simple case, where domain registries require registrants to provide their BusinessID and offer this as a part of their WHOIS information, businesses would not need to exercise any additional efforts to be reliably identified by others.

The two-step process does not suffice for businesses that have registered more domains or have a presence at more locations, such as market places or social media. Also in most cases basic identity is not sufficient to facilitate user trust. This will typically require demonstration of one or more third party claims. Finally a third step may be used by the business to provide universally discoverable self asserted information about itself and its services, e.g. a public version of the data it provides to proprietary platforms.

The case examples below aim to be non-technical, merely indicating how the various requirements may be supported. Basic elements of the OpenDiscovery protocol, resolver, and a simple extension for Chrome have been developed as a simple Proof of Concept. The PoC is described at the OpenDiscovery website in more detail [29] to inspire an upcoming more comprehensive discussion of functionality and specifications between interested parties.

1. *The business has a multitude of registered domains and URL endpoints.*

While increasing numbers of business registries can be expected to support the entry and listing of an online address, it will typically be limited to one such address. If the domain in question is the primary domain of the company, basic verification is based on the first two steps of the depicted discovery process. Verification of additional domains or URL's claimed by the business requires use of a third resolver step where the business entity can provide claims about such additional domains. The precise location of such claims are discovered via .wellknown (or DNS) based on the primary domain listed in the business registry. Once a domain or a URL matching the one from which the resolved BusinessID was originally retrieved, the resource ownership is validated.

The resolution protocol may even be implemented in a way that lets businesses that are not domain registrants, but are associated with more marketplaces and social networks to use an external discovery service provider, which could likely be an existing marketing service provider.

2. *Discovering verified or verifiable claims*

Just as the third step in the OpenDiscovery resolver can be used to locate claims by a business that it controls additional online resources, it can also be used to exhibit references to verified (by certificate) or verifiable (by API endpoint) third party claims about the business. This mimics the physical "certificate walls" previously found in many traditional artisan workshops.

This allows OpenDiscovery resolution to meet requirement F) as stated in Section 3.1.

Similar ideas for discovering such claims via DNS, .wellknown, or presenting them via a JSON Web Token have recently been published [30] by Ryan Sleevi from Google based on consultations with DG CONNECT that is responsible for the eIDAS Regulation.

Specific methods to process such claims are thus also out of scope for this paper. It is envisioned, however, that the methodology and syntax currently being developed for discovery of 3. party claims between existing and (potentially) new members of a federation "OpenID Connect Federation 1.0" [31] might serve as a starting point for developing such methods.

3. *Making the Business and its services universally discoverable by user agents*

The original incentive for businesses to market services via their own website was to become easily discoverable and trusted by potential customers. As long as there were only a few businesses online in each product category users could easily conduct manual searches and make proper choices as search engines were free and unbiased. Search engines even developed markup ontologies like schema.org to make webpages more accessible by search bots.

In todays world, where proprietary market places, price comparison services, and business/service directories are challenging the open web, this has largely changed. The machine readable web has degenerated into a number of data feeds made specifically available for individual proprietary marketing and sales channels. Businesses have become the underdogs in the interaction with a number of infomediaries that increasingly limit the information available to consumers using excessive charges to allow only data from the highest bidders to pass the information barriers between businesses and customers.

The newly proposed European Data Strategy [32] challenges this kind of data flow restrictions:

> Citizens should be empowered to make better decisions based on insights gleaned from non-personal data. And that data should be available to all – whether public or private, big or small, start-up or giant. This will help society to get the most out of innovation and competition and ensure that everyone benefits from a digital dividend. This digital Europe should reflect the best of Europe - open, fair, diverse, democratic, and confident.

This open and fair data sharing cannot be enabled without a consistent and scalable basis for identification of businesses, facilitation of trust, and discoverability of their data. Data about offered services and corresponding needs (“supply and demand” data) will be the natural first priority for such sharing.

To realize such general business data discoverability, it is essential that everyone can easily discover relevant business entities and any data they decide to make available. For this purpose it is not sufficient to be able to make simple lookups in business registries. To search openly for businesses it will be essential that business registries allow bulk downloads of core business data, either for all businesses or for specific types, e.g. based on location or NACE code (= business segment). Fortunately this is already possible in many jurisdictions and will be mandated in the EU from mid 2021 by the Open Data Directive.

The ability to make their data more easily available to any interested user agent is ultimately where the OpenDiscovery value proposition will be for most businesses. Short-term, it can be used to develop simple purchasing agents that will assist users in finding and selecting products based on user preferences and terms rather being biased by infomediary interests. Long-term, it is expected that user agents develop into more autonomous AI agents, that may assist individuals in dealing with the growing number of AI assisted sales agents run by platforms and businesses.

These options fit well with the MyData mission of empowering citizens to thrive in upcoming data-driven ecosystems. MyData Global has received specific mention in the EU Data Strategy proposal and has recently issued a white paper [33] outlining how “MyData Operators” – a new type of user agent – may develop in order to ensure the empowerment of individuals in the data driven economy.

This will allow OpenDiscovery resolution to meet requirement G) to H) as stated in Section 3.1.

3.4 Bootstrapping and fallback mechanisms

Despite the market leading efforts among business registries in the EU and TLD registries in the Nordics, it may take considerable time before full automation is supported by enough business registries and TLD registries to reach a tipping point for becoming a global standard. Therefore, bootstrapping as well as fallback mechanisms are needed to support gradual adoption and transition.

Fortunately there are opportunities not only for implementing such mechanisms, but also to do it in ways that may benefit the existing CA ecosystem significantly in the transition period. The current problem is that the EV certification market has never taken off, and without a widespread identity assertion mechanism for businesses, there has been no basis for establishing any trust mechanisms.

Whitelisting of well known major business entities and websites

One of the primary issues with EV Certificates has been the missing use of EV certificates by most internet giants. On this basis, many lower ranking companies have decided to similarly dismiss the use of EV certificates. With OpenDiscovery the responsibility for the authentication of businesses shifts from the business side to the user side. This has the profound effect that resolvers and agents trusted by their end users can bootstrap the ecosystem by whitelisting an exhaustive list of major wellknown businesses and their primary online resources. This may readily allow a shift from positive or neutral indicators to providing clearly negative indicators for non-identifiable businesses, which will significantly strengthen the motivation of these businesses to become identifiable. The whitelisting feature must of course be implemented to be automatically overridden by any claims provided by the entities themselves. Specifically in enterprise environments, it would also be possible for the individual enterprise to easily whitelist any known customer, supplier, and partner domains.

This allows OpenDiscovery resolution to meet requirement I) as stated in Section 3.1.

Fallback using EV certificates – and in particular Certificate Transparency

When business registries do not support entry and readout of an online address (domain or URL) the use of EV certificates is an obvious fallback solution for businesses to assert claims that they control the domain. This means that the resolver should look for EV certificate information in the absence of claims provided directly from the registry data.

The use of OpenDiscovery resolution even provides a number of additional benefits compared to the traditional use of EV certificates:

Businesses with more domains and/or URL-based resources will only need to purchase an EV certificate for one domain and still be able to assert claims regarding their remaining resources.

Discovery of EV certificates via Certificate Transparency [34] logs further allows businesses to enjoy the full range of OpenDiscovery advantages specified in Section 3.1. Specific examples of such advantages include:

a) Businesses can use ACME based DV certificates on all their servers, and rely on all of the price tiers of popular DDOS and WAF-services such as Cloudflare while being identified on the basis of a CT logged EV Certificate that may not be used on any server

b) Certificate Transparency logs may be used to create BusinessID indexes pr. registry, so that registry data can be systematically retrieved even from registries restricted to simple lookups and combined with other resolved claims for use in advanced user agents (*re Req. G) to H)*)

Fallback using data from GLEIF or licensed directories

In jurisdictions where business registries still limit public access to registry data, this often relates to their historic relationships with a number of local directory or business intelligence services. In many cases business data are now freely available through these services. Also the GLEIF database may contain relevant data about LEI registered businesses. OpenDiscovery resolution may thus benefit from looking up data from such proxy services when direct access to registries is limited.

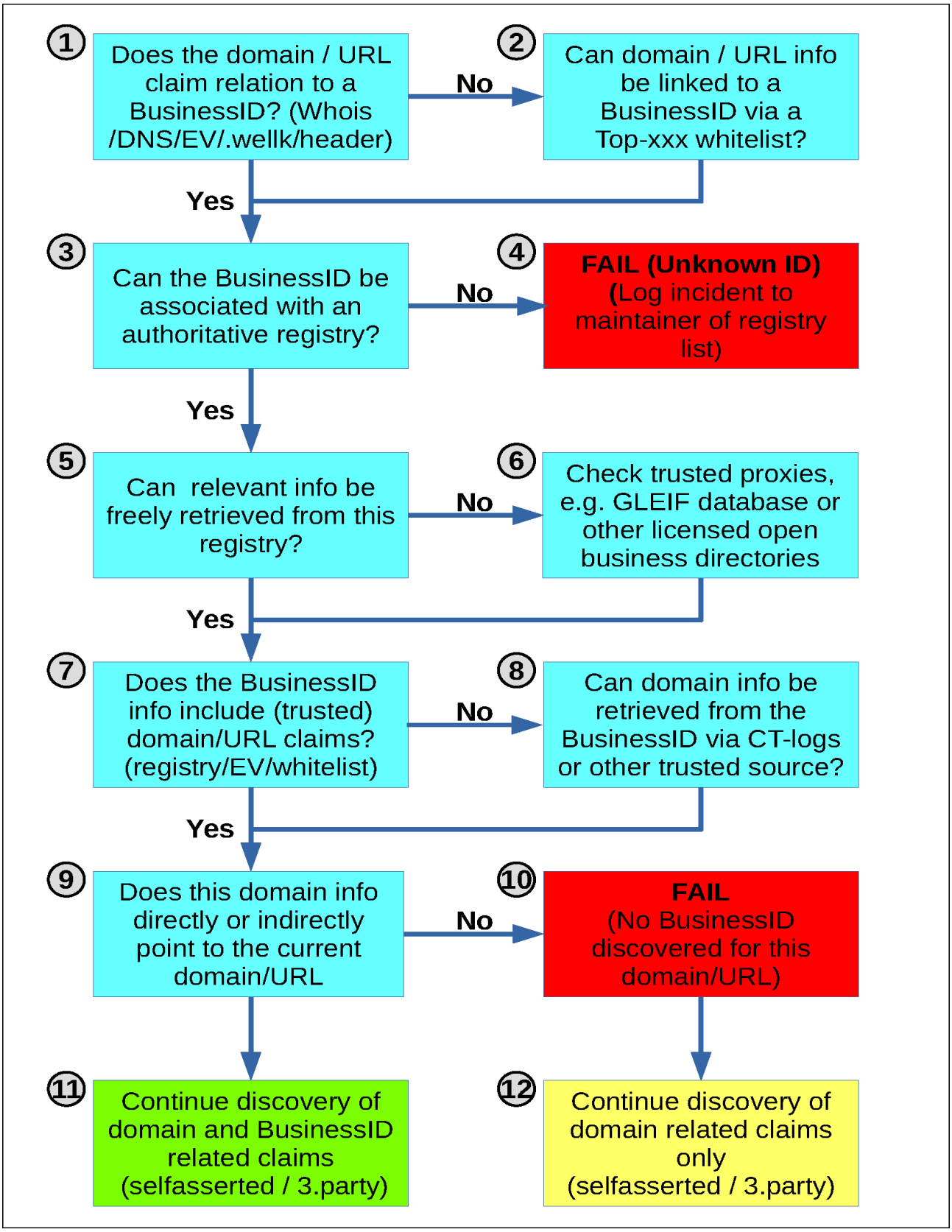

Illustration 4: Rough outline of the resolver process including bootstrapping and fallback options

Trust in such proxy services, however, requires confirmation that the data retrieved are indeed up-to-date copies of authoritative registry information or aquired using strict identity validation of the source. For GLEIF this is supposed to be the case for business records containing a ”fully corroborated” label, but unfortunately there has been problems [35] with mis-labeling in the past.

Extending the ACME protocol to manage issuance of EV Certificates

Even though OpenDiscovery client side real-time validation has inherent advantages to embedding the identity validation in the TLS certificates, it may increase adoption and awareness within the existing certification ecosystem if the ACME protocol could be extended to automatically provide EV certificates or similarly classified certificates in cases where the business registry contains a fully qualified domain name reference and the matching BusinessID is present as part of the WHOIS information from the TLD registry or provided in a specific way in the DNS record of the domain. The latter would require specification as a new verification method by the CA/Browser Forum, but would appear to be a more secure alternative to some of the current DNS based methods of placing a contact email address or a contact telephone number in the DNS and then rely on the integrity of these communication endpoints as well as on the multiple layers of alleged business representatives, lawyers and more.

3.5 Credible claims providers

Having introduced CT-logs to bootstrap the separation of duties between PKI certificate issuers, identity claims providers, and user side identity verifiers it also natural to consider engagement of alternative identity and trust claim providers that have closer or more sustainable relationships with businesses and/or their customers than CA’s. Examples of such possible alternatives or suplements to CA’s as verifiers of the relation between businesses and their online resources could be:

1. ***Local TLD registries***
   National TLD’s in several countries now want to regard themselves as part of the solution to various online security problems, including phishing. Solid verification of registrant identity using national eID’s is an element in their efforts to address this. Another is the inclusion of the BusinessID as part of the WHOIS information which makes the verification resistant to spelling variations and name changes. Depending on the assurance level obtained, WHOIS information could either qualify as identity verification by itself or complement other types of verification to provide additional assurance.

2. ***Banks and Insurance companies***
   The use of documentation from banks is already an optional partial element in EV certification. In many countries banks have lately become subject to strict KYC and AML procedures, including identity verification of persons as well as businesses. In addition to the legally mandated customer assessment, the competivity of a bank strongly depends on customer risk assessment. They have the advantage compared to CA’s that they typically operate in the same jurisdictions as their clients and have stronger relations to their clients than CA’s have.

3. ***Business associations***
   A blog entry hosted by the CA Security Council [36] is only partly right when stating: *”Just because a threat actor could buy an EV certificate for fraudulent purposes, doesn’t mean they will. The goal isn’t to make something 100% hack-proof. The goal is to make hacking and social engineering cost and time prohibitive for threat actors”*. The problem is that this cost and time makes buying an EV certificate even more prohibitive for many small or medium sized

businesses. So the trick is rather to bind the certification to costly activities that ”normal” businesses find attractive, while being useless to imposters. Business associations that offer valuable services to their members and charge large and progressive membership fees could be well positioned as candidates for producing identity related claims.

4. ***Directory Services***
   The value of a directory service is directly proportional to the number of new customers it may attract. This goes for regular businesses as well fraudulous actors. So generally traditional directory services based on selfasserted claims from businesses are not suited as claims providers. Exceptions could be directory services with a clear aim to build and maintain a high level of reputation among the individual users of their services. It will be interesting to see if any services like ”Google My Business” that are currently focused on local trade will develop to support the current shift towards online trade by providing relevant identity and trust assurance.

   In some cases directory and business information services are based on direct feeds from business registries that are unavailable for ad hoc access. Such services often offer free access to large amounts of data to attract customers to additionally purchase value added services such as credit rating reports. Such directory services may be relevant proxies for identity related claims.

5. ***Graph information from major internet platforms***
   As illustrated by the ABNAMRO example in Section 2.3 credible identity does not need to be based on claims from single entities, but may equally well be based on mass aggregation of identical claims or so-called graph data structures, that can serve to document a wider societal acceptance of a claim, normally based on some kind of efforts by the original claimant. The possibility offered by this proposal to authoritatively assert the relationship between a business and its presence on various platforms can make such graph based claims even more valuable for distinguishing between a wellknown business entity and similarly named fraudulous entities.

6. ***Using more verifiers for added assurance***
   The ability of a user or its user agent to verify the identity of a business based on claims from several third parties can provide added assurance for users beyond plain phishing attacks. An example of this could be the following combination:
   a) Basic mutual assertions between a business (BusinessID) and its domain (re. Section 3.2)
   b) Matching information from the TLD registry of the domain registrant (BusinessID)
   c) A bank API (or certificate) allowing confirmation of the match between the BusinessID and a provided account number

   While an attacker compromising the website may replace claim a) with a different claim, the user agent will detect this from the mismatch with claim b). Similarly an attacker trying to link the business/website to a different bank account will cause a detectable mismatch with either claim a) or claim b).

   Similarly an identity profile may be strengthened by supplementing it with claims from relevant social networks or recommender services.

In summary it may be concluded that there are several options to use third party claims about a business, about its registered domains, and about the relation between these to further strengthen the identity verification mechanism described in section 3.2 as well as to provide backwards compatibility for businesses and domains associated with less developed registries. To broadly support such options, however, a generic discovery mechanism for such claims is needed.

4 Summary, status, and recommendations

The purpose of this discussion paper has been to provide an overview of the problems seen with the currently established methods and ecosystem for ID verification of Business entities, and express relevant requirements and solution options to overcome these problems.

While identification of individuals has received widespread attention and is subject to countless innovative efforts, the importance of business identification has been largely overlooked. This is in stark contrast to the physical world, where businesses spend large sums of money on monumental buildings to display their economic capacity and supposedly related trustworthiness, while people have been able to interact almost anonymously with most businesses.

The CA/Browser Forum was created at a time where there was still a broad belief that the internet infrastructure could support free and open B2B and B2C markets, and that reliable identification of businesses would be a base for that. It must now be concluded that this joint ambition failed, but considering the digitalisation state of Business registries and TLD registries at the time, it was also an extremely challenging journey that the CA/Browser Forum embarked on.

In the meantime more proprietary alternatives have emerged, as consumers really do not bother about business identification when buying goods and services on the internet, but only about choice and accountability which is what market platforms now offer – ultimately without regard to whether the suppliers are formally registered with a business registry somewhere in the world.

The paper therefore sets up a list of requirements that must be met if the ecosystem consisting of CA's, user agents, business registries and TLD registries has any intention of providing a base layer for identity, discovery and trust that may challenge the two-sided market place and advertising platforms with their own integrated identity/discovery/trust mechanisms.

Meeting these requirements universally and short-term is quite impossible. So instead a ”Think Global, Act Local” principle is suggested that acknowledges that business registration practices vary considerably across the globe, but still aims to ensure opportunities for businesses in all jurisdictions to participate. But for every kind of provider in the ecosystem it is time to think about what they can do to bring us closer to a joint goal. In most cases it is certainly neither rocket science nor blockchains that are needed, but rather adoption of new business practices that are not requiring substantial technological efforts.

In each of the three camps of the ecosystem (CA/Browser Forum; business registries; and TLD registries, however, we have seen both innovative moves and clear examples of resistance to change.

Within the CA/Browser Forum innovative members like LetEncrypt and Buypass have adopted the ACME protocol to offer free DV Certificates to businesses. Widespread adoption of TLS is a prerequisite for any identity assurance efforts. On the other hand other CA's seem so narrowly focused on selling ”green labels in browser address bars”, that they seem to totally ignore the logic behind browser vendors recent demotion of EV indicators [37] and the vast problems and insufficiencies with EV certificates as described in Section 2 of this paper.

The original rationale for granting limited financial liability to some types of corporations was to facilitate risk taking and innovation within the corporations, but balanced with requirements for transparency allowing investors, suppliers, and customer to assess the financial risk of engaging with them. This transparency has become even more important with the globalization of trade.

Some business registries – with the UK Companies House and the Danish VIRK registry in the lead – have taken this need very seriously, providing detailed current and historical records of business activity. Several other business registries have now also gone public with data and have allowed businesses to register online addresses as well as physical addresses.

In many other jurisdictions, however, business registries may have replaced traditional file cabinets with digital solutions, but their business conduct has remained unchanged over the last decades. Many of these registries prefer to finance their operations by reselling their data to select third parties or to endusers via complicated purchase solutions rather than to facilitate transparency and trust in their registered businesses. This has been the case for the business registries in several countries like Sweden (Bolagsverket, Skatteverket) and Spain (Colegio de Registradores) where you have to visit private proxies as https://www.allabolag.se and http://www.infocif.es/ respectively to access rich data about all businesses free of charge. Similarly in The Netherlands (KVK) data, that should be freely available from the registry are instead monetized via KVK's engagement as an LEI issuer with GLEIF. There are, however, indications that at least Bolagsverket and KVK are getting ready to comply with the impending implementation acts for the EU Open Data Directive.

Similarly there are significant differences between the practices of different TLD registries. The Finnish Traficom (.fi) includes business registrant info including the internationalized BusinessID, while DENIC (.de) has implemented a reverse GDPR protection that intentionally hides the identity of business registrants to prevent individuals from being able to file GDPR complaints and insight requests towards .de domain registrants and operators.

Within the CA/Browser Forum Google has been the main driver in the discussions on EV improvements. In relation to its search and advertising engine, however, Google is using a range of alternative tools, including "Seller Ratings" based on collaboration with review services [38] and "Google My Business" linking websites to verified local businesses [39], and lately "Advertiser Identity" [40] while apparently not weighing in on EV based formal identity as a search ranking property. From a user perspective this "too little – too late" EV support reduces the effect and value of EV based identity provisioning and any possibly linked additional efforts to facilitate informed end user trust evaluation and choice.

It is unclear whether other browser members of the CA/Browser Forum have any ambitions to develop their user agents to better match user needs in a world where the amount of data have effectively outgrown the ability of end users to browse through all options for engaging with businesses. If so, solid options for discovery and identification of businesses and their merits could serve as an attractive foundation for implementing content filtering based on user preferences rather than advertising engine economics.

This paper will conclude by giving some general recommendations as well as some suggestions for specific collaborative action that may be used as a starting point for a wider dialogue. A dialogue which must focus on how to advance from the current global failure for adoption of business identity verification towards a solution that is attractive for both businesses, individual end users, and innovative service providers.

4.1 High level recommendations

The recommendations given here aim to stop focusing on current operational conflicts of interest and direct the focus towards sustainable end goals and on how these may be achieved gradually at different pace in different jurisdictions via adaptation of the various ecosystem participant roles.

Use proxies to solve practical problems – not to challenge the primary authorities

There can be many and good reasons to establish proxies for identity authorities. Most importantly where the business model or legal regime under which an authority operates is not facilitating open access to relevant identity attributes. Facilitation of open public access to data is generally of great value to businesses that are subjects to such ”closed data” authorities.

As the discussion in this paper has shown, however, proxies that operate as a service for the provider side are likely to favour the interests of their clients or sponsors rather than interests of the parties that rely upon and need to trust the data. From a relying party perspective it is therefore essential to be able to decide on which supplier side proxy to trust – or to take the more difficult path of obtaining the required data directly from or attested by the relevant authority.

Unfortunately proxies operated by independent entities also have a tendency to strive towards becoming separate authorities. This has been seen with EV Certificates, where CA’s simply verify associations between legal entities and internet domains, but have been falsely claiming that such verifications should inherently facilitate trust among relying parties not even knowing the CA. EV certificates – and even the newer EU eIDAS QWAC certificates – are issued without proper delegation of authority from the real authority. And even without reference to the proper authority apart from a local registration number that leaves the relying party with a partial identity claim: ”someone (guess who by solving the number riddle) authorized this entity to operate as a business” signed by someone they have never heard of. How would that approach work for passports, drivers licenses, vehicle and animal registrations, university degrees and so forth?

GLEIF is another example of such a proxy mechanism. It has made valuable achievements to the transparency of financial transactions by locating various national and local business registries and providing public access to business data not otherwise easily accessible. But as business registries increasingly make updated information directly available, the static proxying in the LEI register becomes a problem rather than a benefit – and is perceived by businesses as a fully unnecessary cost and administrative burden. At the same time many LEIs issued to businesses in jurisdictions with ”closed” business registries are based on data wholly or partially asserted by the requester rather than being acquired from the business registries. The Financial Stability board has recently issued a report [41] adressing these challenges for GLEIF. To a wide extent, however, this report also features GLEIF as an organisation seeking new problems to solve. This view is underpinned by a GLEIF use case vision presented in a CEN/CENELEC report on Distributed Ledger/Blockchain Technologies [42] and embodied in a collaboration with the Ethereum based blockchain uPort [43] with an unclear purpose of creating a new centralized identity management solution for businesses without clarifying its relationship to the actual authoritative business registries.

The recommendation here is that identity proxies focus their activities on assisting individual businesses with aquiring, maintaining, and presenting verified or verifiable claims from the real authorities similar to the idea behind the W3C Verifiable Credentials for individuals [44], leaving the verifier role to the relying parties (here: customers of the business) or their chosen agents. The current technical and practical experience of proxies could be utilized to offer such modern digital services as a service to business registries rather than acting independently of these.

Strive for transparency and collaboration

A major reason that the internet is still missing a basic way for businesses to be discovered and identified is missing or insufficient dialogue between the various stakeholder groups involved. And because some stakeholder groups have been focusing too much on their own short term options rather than focusing on the overall societal problem to solve. As an example, in the EU there are major inconsistencies even between the high level political aims expressed in the recent Data Strategy proposal, the options for managing business identity in the eIDAS regulation, and the way many national business registries are operated. Therefore, establishing and growing a ”coalition of the willing” across all relevant stakeholder groups must be a primary objective.

One of the promises of the internet was the ability to easily share data on a global scale. But so far people and most businesses are not in control about what is made sharable. As regards the use of data for public services, the EU has introduced the ”Once Only” principle [45] to ensure that businesses and individuals only need to provide their information once in order to serve the needs of all public administrations. OpenDiscovery seeks to extend this principle to the private sector allowing businesses to publish relevant information about themselves in an easily and universally discoverable way rather than having to rely on the ”multihoming” effect that EU reports [46] often describe as a problematic alternative to dominant platform ecosystems. This is because these reports focus primarily on enabling secondary use of platform aggregated data with reference to the GDPR data portability requirements, while OpenDiscovery aims at making market data widely and transparently available for first use.

It is recommended that discussions regarding means and roles in relation to implementation of OpenDiscovery involve representatives from government, business registries, TLD registries, user agents providers, proxies, and potential infrastructure providers as well as standards organizations with an aim to facilitate an open ecosystem where businesses can manage their own identities as well as transparently exhibiting their product and service offerings.

”Think Global – Act Local”

A major obstacle to the development of business identity in pace with technology is the radically different degree of readiness in different juridictions for public services to cope with change. To create more rapid progress it will be necessary to replace the ”One Size Fits All” approach with a ”Think Global – Act Local” approach. As with the shift from ”http” to ”https” the important point is to reach a tipping point in adoption that allows a shift from positive indicators for compliance to clearly negative indicators for non-compliance. With the exception of a few global actors, the markets for consumer products and services are still dominated by national and regional businesses, while most fraudulous actors reside in other areas. The combination of a whitelisting option for major businesses and automated verification of the many smaller businesses using local TLD’s makes it realistic to rapidly reach the tipping point in the countries that have been mentioned as leading examples. As the Open Data Directive gets implemented throughout the EU and the benefits of OpenDiscovery in the initially supported countries can be demonstrated, the tipping point may gradually be reached in the remaining EU countries.

So far many technological and practical advances introduced by major platforms have been launched initially in the USA. But business registration in the US tends to be more complex and most business registries in the US are lagging behind their European counterparts. Importantly, a decentralized business identity ecosystem will also match the needs of the EU Data Strategy while challenging the interests of the major US platforms. So developments as outlined will most likely need to be driven from the EU joined by participants from various other parts of the world.

4.2 Initial discussions and actions

The author of this discussion paper will initially seek to engage in dialogues with representatives for each of the individual stakeholder groups that have been addressed in the paper. In particular, this will include the following groups:

CA/Browser Forum members and other identity proxies

CA's and browser vendors jointly represent a longterm expertise in providing business entities with identity claims. While the OpenDiscovery method proposed in this paper may be implemented without the cooperation of proxies like the CA/Browser Forum and GLEIF, it would certainly benefit from a broad and synergetic collaboration with these parties. Questions to be addressed will as a minimum include:

- Is there ambition to engage in efforts that may lead to a tipping point for business identity verification similar to what has been experienced for integrity and confidentiality (TLS)?
- Can CA's see opportunities shortterm (higher EV sales) – as well as longterm (e.g. offering CA services to various "real" authorities)?
- Can browser vendors see opportunities shortterm (trust) and longterm (service discovery)?
- Could GLEIF and/or CA/Browser Forum members envision a further development of the current registry lists to be used as a basis for implementing a general BusinessID resolver? Can agreement be reached regarding an internationalized BusinessID of global reach?
- Could CA/Browser forum envision an ACME protocol extension or a separate protocol / guideline to support automated EV certificate issuance for businesses in supportive jurisdictions? What would be the major concerns?
- Are there any concerns or improvement suggestions to the proposed method of automation, bootstrapping, and the fallback role for EV certificates using certificate transparency logs?
- Is there an interest to participate in the work to identify relevant standards and supplementary needs for standards, guidelines and schemas?
- Could there be synergies with OpenCorporates who has developed proprietary data grabbers for a large number of registries, but for a more specific investigative purpose?

Business Registries and EU bodies

Business registries are the authorities for the legal existence of businesses and thus the primary stakeholder group to involve. It is important to understand any motives many registries have had to conceal information from the public despite the original purpose of ensuring transparency against limiting the liability of some types of corporations. Questions for business registries include:

- How do registries see their role in relation to facilitate trust through transparency with the businesses in their registries? How do EU registries plan to comply with the implementation acts for the Open Data Directive?
- What are the considerations related to supporting URL entries in business records?
- What specific plans are there for offering data as a response to individual lookup requests?
- What specific plans are there for offering bulk access to registry data?

TLD Registry Operators

Although TLD registry operators have authority for the delegation of fully qualified domain names under their TLD, their direct support for registrant information and validation is not as critical for the implementation of OpenDiscovery as the support by business registries. This is because there are alternative ways for registrants to assert their control over a domain. However, support for BusinessID (or a uniquely resolvable business name) in the WHOIS record enables fully inherent and automated identity verification of businesses. Questions for TLD registry will include:

- What is the status and plans for offering secure and internationalized WHOIS lookups including registrant name for legal entities?
- Does the registry apply or plan to apply an identity verification proces for new business registrants?
- How does the registry regard the option – as now introduced by several registries – of providing the internationalized BusinessID as part of WHOIS for registrants that are legal entities? Could it strike the balance between privacy and transparency that has been discussed since the introduction of the GDPR?

Potential user agents and aggregation resolver operators

The purpose of providing open source OpenDiscovery components including a full resolver is to ensure that it may be easily implemented by multiple parties. This will allow end users to decide for themselves which resolver operator to trust. Implementations may range from ambitious resolver operators wanting to support a wide range of businesses worldwide, to more targeted implementations focusing on specific jurisdictions and/or product and service types. Efforts will be done to explore likely types of candidates, whether these would be focusing on facilitating trust in already discovered business entities or have a wider ambition to facilitate product/service discovery.

Corporations and SME's

Businesses generally do not see customer trust and security as a goal in itself. The primary value proposition for businesses will be to offer them better chances of being discovered and selected by customers and at a lower cost than using current search engines and market places. Initial efforts will focus on defining attractive transitioning paths towards disintermediation of these actors. A major desire among many businesses is a broader access to data about supply and demand within their respective markets. This is fully consistent with the objective of the proposed EU Data Strategy and will become the focus for the dialogue with consumer facing corporations and SME's. Part of this dialogue will be conducted within the MyData Global community that is currently looking into business models that support the emergence of a new breed of MyData Operators ("user agents") in order to empower end users to make informed decisions and to share data more efficiently with businesses.

Standardization needs

Existing standards and guidelines relevant to OpenDiscovery are dominated by IETF (RFC's) and CA/Browser Forum Guidelines. Related identity management standards have been developed (or are under development) by the OpenID Foundation and W3C. A dialogue will be initiated to assess the options to integrate OpenDiscovery specifications with existing or planned work items or to create a specific new work item within one of these organizations.

4.3 Open invitation to engage

The implementation of the ideas put forward in this proposal require wide collaboration between various types of actors. Anyone agreeing to the need for businesses to verify their online identities and make their services and merits more easily discoverable are strongly encouraged to share their concerns or suggestions for improvements to the proposed OpenDiscovery method.

By intention this paper has avoided any detailed proposals for technical implementation apart from referencing relevant existing technology and standards in broad terms. Alternative proposals to obtain similar advances relative to the current state-of-the-art as well as more technically specific implemention proposals are also welcome.

The current very basic technical description and initial Proof of Concept is available here and will be further developed based on suggestions and collaborative efforts:
https://www.opendiscovery.biz/

The author may be contacted via email: hb@peercraft.com or via LinkedIn:
https://www.linkedin.com/in/hbiering/

5 References

1. **Google: This surge in Chrome HTTPS traffic shows how much safer you now are online**
   Liam Tung; ZDNET [2017-10-23]
   https://www.zdnet.com/article/google-this-surge-in-chrome-https-traffic-shows-how-much-safer-you-now-are-online/

2. **Moving towards a more secure web**
   Emily Schechter; Chrome Security Team [2016-09-08]
   https://security.googleblog.com/2016/09/moving-towards-more-secure-web.html

3. **A milestone for Chrome security: marking HTTP as “not secure”**
   Emily Schechter; Chrome Security Product Manager [2018-07-24]
   https://www.blog.google/products/chrome/milestone-chrome-security-marking-http-not-secure/

4. **Extended Validation not so... extended? How I revoked $1,000,000 worth of EV certificates!**
   Scott Helme [2019-09-11]
   https://scotthelme.co.uk/extended-validation-not-so-extended/

5. **Chrome’s Plan to Distrust Symantec Certificates**
   Devon O’Brien, Ryan Sleevi, and Andrew Whalley; Chrome Security [2017-09-11]
   https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html

6. **Cyber-Mercenary Groups Shouldn't be Trusted in Your Browser or Anywhere Else**
   Cooper Quintin; Electronic Frontier Foundation [2019-02-22]
   https://www.eff.org/deeplinks/2019/02/cyber-mercenary-groups-shouldnt-be-trusted-your-browser-or-anywhere-else

7. **Phishing with EV** (2 parts: First and Final)
   James Burton [multiple edits 2017 - 2018]
   https://www.typewritten.net/writer/

8. **Extended Validation Certificates are (Really, Really) Dead**
   Troy Hunt [2019-08-13]
   https://www.troyhunt.com/extended-validation-certificates-are-really-really-dead/

9. **Why Are You Removing Website Identity, Google and Mozilla?**
   Tim Callan and Kirk Hall; Sectigo, Entrust Datacard [2019-08-27]
   https://casecurity.org/2019/08/27/why-are-you-removing-website-identity-google-and-mozilla/

10. **The Web’s Identity Crisis: Understanding the Effectiveness of Website Identity Indicators**
    Christopher Thompson, Martin Shelton, Emily Stark, Maximilian Walker, Emily Schechter, and Adrienne Porter Felt; Google [2019-05-31]
    https://www.usenix.org/system/files/sec19-thompson.pdf

11. **We exist to make the world’s company data open for all**
    Opencorporates [as pr. 2019-09-18]
    https://opencorporates.com/info/about/

12. **When to use Extended Validation SSL**
    Digicert [undated]
    https://www.digicert.com/when-to-use-ev-ssl.htm

13. **Guidelines For The Issuance And Management Of Extended Validation Certificates, Version 1.7.2**
    CA/Browser Forum [2019-12-19]
    https://cabforum.org/wp-content/uploads/CA-Browser-Forum-EV-Guidelines-v1.7.2.pdf

14. **Intent to Deprecate and Remove: Trust in existing Symantec-issued Certificates**
    Ryan Sleevi (Google) [2017-03-23]
    https://groups.google.com/a/chromium.org/forum/#!topic/blink-dev/eUAKwjihhBs%5B1-25%5D

15. **EU shrinks tax haven blacklist, removes UK, Dutch territories**
    Francesco Guarascio, Reuters, [2019-05-17]
    https://www.reuters.com/article/us-eu-tax-blacklist/eu-shrinks-tax-haven-blacklist-removes-uk-dutch-territories-idUSKCN1SN12M

16. **Offshore Leaks Database: Quovadis Limited**
    Sourced from Paradise Papers – Appleby [2014]
    https://offshoreleaks.icij.org/nodes/82004660

17. **Public Disclosure of External Issuing CAs**
Quovadis Limited [undated, as pr. 2019-10-09]
https://www.quovadisglobal.com/QVRepository/ExternalCAs.aspx

18. **Accreditation: WebTrust for Extended Validation**
Quovadis Limited [undated]
https://www.quovadisglobal.bm/Corporate/Accreditations.aspx

19. **EV Certificate used for quovadisglobal.bm**
Quovadis Limited [BM] [undated, as pr. 2019-10-09]
https://crt.sh/?q=92ed077d51317ddf9025c04f937c0ba6b7f3a66e

20. **A Complete Study of P.K.I. (PKI's Known Incidents)**
Nicolas Serrano, Hilda Hadan, and L. Jean Camp, Indiana University - Bloomington [2019-09-26]
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3425554

21. **Including LEIs as extensions in EV certificates**
Cabforum mailing list discussion initiated by Stephan Wolf, GLEIF [2019-09-22]
https://cabforum.org/pipermail/validation/2019-September/001325.html

22. **Business Registers Interconnection System (BRIS)**
The European Commission
https://e-justice.europa.eu/content_business_registers_at_european_level-105--restore-en.do

23. **Open Corporate Data in jurisdictions around the world**
OpenCorporates [undated]
http://registries.opencorporates.com/

24. **Directive (EU) 2019/1024 on Open Data and the re-use of Public Sector Information**
The European Parliament and the Council of the European Union [2019-06-20]
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L1024

25. **Number of companies pr. jurisdiction registered with website address**
OpenCorporates [undated]
https://opencorporates.com/companies?jurisdiction_code=&q=&utf8=%E2%9C%93&types_of_data_held=Website

26. **GLEIF Registration Authorities List**
GLEIF [undated]
https://www.gleif.org/en/about-lei/code-lists/gleif-registration-authorities-list

27. **Making progress on disclosures of data sources**
Ryan Sleevi, Google [2020-04-10]
https://cabforum.org/pipermail/validation/2020-April/001441.html

28. **DigiCert Legal Repository - Approved Incorporating Agencies**
Digicert [2019-12-06]
https://www.digicert.com/legal-repository/ (Select "Approved Incorporating Agencies")

29. **OpenDiscovery**
Henrik Biering (Peercraft) [2017 – 2018]
https://www.opendiscovery.biz/

30. **Soliciting feedback on potential changes to Qualified Website Authentication Certificates**
Ryan Sleevi, Google [2020-01-14]
https://cabforum.org/pipermail/servercert-wg/2020-January/001555.html

31. **Federations - trust between entities**
Andreas Åkre Solberg and Roland Hedberg et al. [2019-11-07]
https://openid.net/specs/openid-connect-federation-1_0.html

32. **European data strategy**
European Commision [2020-02-19]
https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy

33. **Understanding MyData Operators**
MyData Global, joss Langford, Antti 'Jogi' Poikola et al. [2020-04-29]
https://mydata.org/

34. **What is Certificate Transparency?**
Google [undated]
https://www.certificate-transparency.org/what-is-ct

35. **Global LEI System Business Report Q3 2018**
GLEIF [2018-11-06]
https://www.gleif.org/content/4-lei-data/2-global-lei-index/2-download-global-lei-system-business-reports/20181106-download-global-lei-system-business-report-q3-2018/2018-11-06_quarterly_business_report.pdf

36. **The Insecure Elephant in the Room**
Paul Walsh (CEO; MetaCert) [2019-10-10]
https://casecurity.org/2019/10/10/the-insecure-elephant-in-the-room/

37. **Making progress on disclosures of data sources**
Doug Beattie, Globalsign [2020-04-22]
https://cabforum.org/pipermail/validation/2020-April/001444.html

38. **Seller Ratings**
Google Merchant Center Help [undated]
https://support.google.com/merchants/answer/190657

39. **Verify your site ownership**
Google Search Console Help [undated]
https://support.google.com/webmasters/answer/9008080

40. **Increasing transparency through advertiser identity verification**
John Canfield, Google [2020-04-23]
https://www.blog.google/products/ads/advertiser-identity-verification-for-transparency/

41. **Thematic Review onImplementation of the Legal Entity Identifier**
Financial Stability Board [2019-05-28]
https://www.fsb.org/wp-content/uploads/P280519-2.pdf

42. **Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies**
CEN/CENELEC Focus Group BDLT [2018-06-13]
ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Sectors/ICT/Blockchain%20+%20DLT/FG-BDLT-White%20paper-Version1.2.pdf

43. **uPort partners with the GLEIF network to launch decentralized corporate identity management**
uPort [2019-11-05]
https://medium.com/uport/uport-partners-with-the-gleif-network-to-launch-decentralized-corporate-identity-management-2a7a20be3354

44. **Verifiable Credential Data Model 1.0**
W3C Recommendation [2000-11-19]
https://www.w3.org/TR/vc-data-model/

45. **Once Only Principle**
EU TOOP Project [undated]
https://toop.eu/once-only

46. **Competition policy for the digital era**
European Commission (Jacques Crémer,Yves-Alexandre de Montjoye, and Heike Schweitzer) [2019-05-20]
https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf