Towards a secure eID system

Recommendations regarding a secure, universal and open digital eID system for an open, safe and prosperous society

CSR

Cyber Security Council

Cyber Security Raad

Towards a secure eID system

Recommendations regarding a secure, universal and open digital eID - system for an open, safe and prosperous society

Addressed to:

The State Secretary for the Interior and Kingdom Relations
The Minister of Justice and Security
The State Secretary for Economic Affairs and Climate Policy

CSR
Cyber Security Council
Cyber Security Raad

07 November 2019

CSR Recommendation 2019, No. 1

Introduction

Developments in the digital domain offer many economic and social opportunities which can only come to fruition if the Netherlands maintains cybersecurity. The Digital Government Agenda[1] published in 2018 states that it is essential to safeguard the Constitution of the Netherlands and the public values derived from it, such as privacy, self-determination and equality, particularly in light of the ongoing digitalisation. The Agenda addresses both seizing opportunities and safeguarding rights. The Dutch Digitalisation Strategy[2] was also published last year; this Strategy is intended as a means for the Dutch Government to further strengthen the earning potential of the Netherlands and ensure better digital skills and cybersecurity in society. It is important to ensure the preconditions for economic success: the security of, trust in and the reliability of the digital infrastructure. An electronic means of identification (eIDs) is a necessary pillar for achieving those aims.

Broad consensus exists that citizens, businesses and those businesses' employees must be able to log-in to government organisations, service providers, care institutions, online shops, suppliers and so on. A wide range of parties (public, private and non-profit) are working step-by-step to increase the trustworthiness of the available log-in tools and to safeguard continuity so that citizens and businesses can manage more of their affairs online. The efforts of the Dutch government in this regard are concentrated on how citizens and businesses log in in the public domain, but not on how they do so in the private domain. This uneven focus leads not only to fragmentation and confusion, but might also lead to a situation in which privacy and safety are insufficiently guaranteed when logging into businesses and organisations in the private and non-profit sectors, which could potentially allow fraud and misuse to increase and vital digitalisation projects to stagnate.

The digital economy offers major opportunities and possibilities for procuring services and products online. Digital identification, the means to facilitate economic transactions and clarity (including legal certainty) regarding the use of data are essential to the commercial sector in the Netherlands, as they are the pillars for economic growth in the increasingly dominant digital domain. In the physical world, we can hardly conceive of conducting economic transactions without assurances regarding identities, property ownership and who is authorised to do what. Means and organisations exist for this purpose, such as passports and identity cards, the land registry and chamber of commerce, civil-law notaries and municipal service desks. Statutory frameworks and guarantees are in place for each of these structures, for which the government bears heavy responsibility.

In the digital world, by contrast, such broad infrastructure is so far lacking and the necessary assurances are much less self-evident. The digitalisation of transaction processes is proceeding with difficulty, in particular because no flexible eID infrastructure exists for both the public (BSN) domain and the private domain. The government is ceding responsibility not only for the authentication of businesses and their employees to the market, but for the authentication of citizens in the private domain as well. As a result, citizens do not yet have access to a secure, privacy-friendly eID that can be used in both social activity and e-commerce. The question now is whether we in the Netherlands are making sufficient strides towards the realisation of a solid digital infrastructure that can protect citizens and businesses in the digital era and can facilitate economic growth in the subsequent phase of the digital internal European market.

[1] NL DIGIbeter: Digital Government Agenda, Government-wide Digital Government Policy Forum, 2018

[2] Dutch Digitalisation Strategy: *'Getting the Netherlands ready for the digital future'*, Ministry of Economic Affairs and Climate Policy, 2018

The CSR feels that the Netherlands can and must take major steps towards creating a broad, secure and privacy-friendly eID infrastructure. These efforts will unite economic interests with those of national security and the protection of Dutch citizens, businesses and their data. In light of the government's traditional role as an anchor and supplier of the source identities of citizens and businesses, the government can reasonably be expected to lead the way in this area. There is naturally also a task here for the various social organisations that deal with relevant information, including that pertaining to identity.

CURRENT SITUATION: TWO SEPARATE DOMAINS

In the digital world, everything is connected. This basic principle must inform any approach to the creation of a digitally secure infrastructure. Our current identity infrastructure, however, remains divided into two domains: the public (BSN) domain of citizens and governments and the private domain of citizens, businesses and non-public organisations. In the Netherlands, this division is based on the regulations governing the use of the BSN. It is not the CSR's intention to open a debate on this division. The Cyber Security Council does, however, wish to emphasise that this division itself necessitates a flexible eID infrastructure which will make it possible for citizens to submit different personal identifying details under different circumstances for the purpose of authentication, i.e. the BSN in the public domain and other relevant pieces of information in the private domain. This is in keeping with the eIDAS Regulation, which encourages member states to structure and deploy their trust services and infrastructure in such a way that these can also be used for social transactions and activity in the 'marketplace'. See point 17 of the eIDAS Regulation:

> *Member States should encourage the private sector to voluntarily use electronic identification means under a notified scheme for identification purposes when needed for online services or electronic transactions.*

The ambitions of the Dutch government's current eID programme do not yet extend to the facilitation of safe, privacy-friendly digital authentications and transactions in the social (private) domain. The government is focusing primarily on enhancing the trustworthiness of its existing log-in tools and safeguarding the continuity of those means, so that citizens and businesses can conduct secure online transactions with government organisations and care institutions within the public domain. These are vital matters which the council heartily endorses. There is, however, every reason to equip our digital society with a widespread eID system that will provide users everywhere with the same facilities and protection.

The council notes two developments that underscore the urgent necessity of a broad eID system:

Our digital safety is under pressure

The topic of digital identity is of strategic importance to the Netherlands and Europe. Recent publications such as the Cyber Security Assessment Netherlands 2019[3] and the WRR report 'Preparing for digital disruption'[4] show that the scale of the threat posed by state-sponsored actors continues to

[3] Cyber Security Assessment Netherlands 2019, National Coordinator for Security and Counterterrorism (NCTV), The Hague, 2019

[4] Advisory report 'Preparing for digital disruption', Scientific Council for Government Policy (WRR), 2019

grow. Countries such as China, Iran and Russia are operating offensive cyber programmes against the Netherlands. As part of these programmes, these countries are deploying digital resources in order to achieve geopolitical and economic objectives at the expense of the Netherlands' interests. State actors are also attempting to gather detailed information on our businesses and citizens, typically by gaining access under a false identity. In addition, some state actors wish to influence public opinion or democratic processes, and disrupt or even sabotage vital systems. Nation states also spy on citizens. In this regard, we distinguish between the interest of nation states in personal data in general and targeted spying on particular individuals or groups (e.g. dissidents) for purposes such as influencing or intimidating these individuals/groups (among other objectives). The first line of defence against such activity is a solid eID infrastructure that protects not only the public sector but the private sector from unauthorised access.

Our privacy and digital sovereignty are under pressure

The Netherlands is among the top 5 countries in Europe with regard to online shopping[5]. In addition, the Dutch digital infrastructure is strongly dependent on a limited number of foreign organisations who have their own interests in terms of collecting and applying user data. This could potentially render the Netherlands vulnerable. Thus far, national initiatives in the private and non-profit sector that touch on eID have been small in scale and have failed to garner broad support. As a result, it remains unclear to users which applications they can use and whether these meet the relevant security and privacy requirements. Consequently, as it stands now, citizens are still obliged to use the vulnerable system of a user name and password to access nearly every service, which requires them to manually log in using (and therefore disclosing) that same personal information, time and time again. In order to simplify the log-in procedure, many websites offer citizens the option to authenticate their account using one of the major platforms such as Facebook, Apple, Amazon, Google, or – potentially in the near future – Alibaba or Tencent. As a result, these companies possess large concentrations of data belonging to both Dutch businesses and Dutch citizens, which has direct consequences for our privacy and digital sovereignty.

[5] Statistics Netherlands (CBS), Eurostat 2018, https://www.cbs.nl/nl-nl/nieuws/2018/38/nederland-in-europese-top-5-online-winkelen

RECOMMENDATIONS

The Netherlands should be and remain a secure, open and prosperous society. Public confidence in society and social structures is vital to our social and economic interests. Secure identification and authentication, secure log-ins, secure sharing of data and secure electronic signatures, as well as the adequate protection (encryption) of data are part and parcel of the necessary basic infrastructure in today's digital world.

In the physical world, we possess sufficient means and opportunities and the responsibilities of market and government parties are a matter of law established via numerous regulations and authorities. Whether we will prove able to realise the benefits of a digitalising society will depend on how well we safeguard three core themes: safety, privacy and trust. These three pillars are inextricably linked to the role of the government. The Netherlands must make haste to establish a digital eID infrastructure that can be used both publicly and privately. The Dutch government must re-evaluate the stance which limits it to the public eID domain: a strong, broad role for government in management and oversight is urgently desired in connection with the combined public and private use of eID tools. It is the basic conviction of the CSR that as many users must gain access to log-in means rated as *substantial* or *high* (according to the levels established by the EU) as quickly as possible.[6]

The CSR recommends the following perspectives for action:

1. Coordinate and facilitate the development of a universal system for digital authentication, electronic signatures and encryption that will protect citizens and businesses in both the public and social domains (eID system), and in doing so further expand upon the existing expertise in the Netherlands.

2. Choose a decisive public and private approach under government supervision, aimed at realising an open infrastructure (prevent forced choices, i.e. truck system, and lock-in).

3. Encourage the use of secure means of log-in by citizens and businesses in the social domain.

[6] EU Regulation no. 910/2014 of the European Parliament and the Council, dated 23 July 2014, regarding electronic identification and trust services for digital transactions in the internal market and repealing Directive 1999/93/EG, https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32014R0910

Re 1. Coordinate and facilitate the development of a universal system for digital authentication, electronic signatures and encryption that will protect citizens and businesses in both the public and social domains (eID system), and in doing so further expand upon the existing expertise in the Netherlands.

Our country stands to benefit from an integral, widely-shared vision and approach by the government. Secure log-ins, secure sharing of data and secure electronic signatures should be every bit as self-evident in our digital world as they are in the physical world. The CSR therefore calls on the government to, in addition to its current policy, actively and in a coordinating and facilitating role contribute to the development of a universal system for digital identification and authentication (an eID system). The CSR also strongly urges effective alignment with recent eID developments in the Netherlands (at businesses and municipalities, in the care sector, etc.) and in the European Union. The development of the universal system must fit within the frameworks established by the EU. Any obstacles that impede this development – legal and otherwise – must be resolved as quickly as possible, and the government must be more emphatic in prioritising such efforts. This also reflects the content of the recently published Dutch Digitalisation Strategy *'Nederland digitaal - Hier kan het. Hier gebeurt het*'.[7] Where the pillars supporting economic growth are concerned, digital identification, the facilitation of economic transactions and the right to use data are essential and inextricably linked to this strategy. This strategy is intended to further strengthen the earning capacity of the Netherlands and promote improved digital skills among citizens and greater cybersecurity in society. A secure eID is needed as the basis for reliable digital (economic) transactions and for the adequate protection of personal data.

Re 2 Choose a decisive public and private approach under government supervision, aimed at realising an open infrastructure (prevent forced choices, i.e. truck system, and lock-in).

In the physical world, the government's role is clear and the goals (including policy objectives) are set out according to an abstract framework in the form of the social contract. In the digital world, however, no such framework exists. As a result, the distinctions between the respective roles of citizens, businesses and governments are unclear and, unlike in the physical world, there is a lack of governmental regulation in the societal domain. The Netherlands is among those countries at the forefront with regard to cybersecurity. Maintaining our leading position remains a priority and will require a structural focus on our digital infrastructure on the part of our government, politicians, policymakers, boardroom members, supervisory bodies, businesses and citizens. Everyone shares in the responsibility to protect our economy, prosperity and society. A reliable eID system must be a cornerstone of these efforts. This is an area in which the government must lead, including by setting the example. Citizens and businesses must be able to transact safely online with the government. The CSR feels there is a broad social need for the government to extend this responsibility to the private domain.

The government must play a well-considered role in the management and supervision of public interests in order to more firmly embed European values and prevent a disproportionate distribution of power, including digital monopolies. There exists a need for safe, practical and usable means of

[7] Dutch Digitalisation Strategy: *'Getting the Netherlands ready for the digital future'*, Ministry of Economic Affairs and Climate Policy, 2018

identification and authentication which reflect European values – including autonomy, transparency, self-determination and privacy – and which do not increase our dependency on foreign ICT suppliers. The three ministries who each bear responsibility for a portion of the digital society in the Netherlands, namely the Ministry of the Interior and Kingdom Relations (BZK), the Ministry of Economic Affairs and Climate Policy (EZK) and the Ministry of Justice and Security (JenV), should – in cooperation with one another and with the private and non-profit sectors – be able to quickly realise such a universal eID system.

Re 3 Encourage the use of secure means of log-in by citizens and businesses in the social domain.

The General Data Protection Regulation and eIDAS demand security and privacy by design. In order to meet requirements of this nature, appropriate provisions must be made.
Here, too, the CSR emphasises the duties of care (legal and otherwise) businesses have with regard to cybersecurity and data processing.[8]

Only recently did the Ministry of the Interior and Kingdom Relations institute an approval system for private log-in tools used by citizens in the government sphere. This may have a positive impact on the use of similar means in the social-private domain. Yet broad deployment of these means will most certainly not happen by itself: it will require cooperation from the national and international e-commerce sector as well. It is also vital that we be able to identify ourselves safely on foreign websites. This sector must be enabled to provide access to its own services in a safe, privacy-friendly and affordable fashion, so that users are not (by default) forced to log in with another account, such as their Facebook account. These log-in tools must be user-friendly and perhaps even free of charge if they are to effectively compete with the authentication means belonging to the major platforms. This is of strategic importance to the Netherlands. Furthermore, it means that commercial parties who offer products and services online must be involved in the intended cooperation as well. They must be facilitated in offering the secure eID means of authentication to their users. The same rules of play that call for citizens to have control of their data, as described in the 'Vision on Information management' document published by the Ministry of the Interior and Kingdom Relations, should also apply in the private domain.

[8] Cyber security guide for businesses: 'Every business has duties of care in the field of cybersecurity', Cyber Security Council, 2017

TARGETED RECOMMENDATIONS

The recommendations are addressed to:
the State Secretary for the Interior and Kingdom Relations,
the Minister of Justice and Security and
the State Secretary for Economic Affairs and Climate Policy.

The CSR makes the following recommendations.

The State Secretary for the Interior and Kingdom Relations:

1. Lead and supervise the further development of a universal open eID system that also protects citizens and businesses in the social domain.
2. Coordinate and facilitate efforts to deploy trustworthy eID means in the social digital domain in the near term, in order to enable secure authentication, signatures and encryption in this domain as well.
3. Facilitate the development of trustworthy eID means in such a way that the right to privacy, autonomy and self-determination remain key priorities.

The State Secretary for the Interior and Kingdom Relations,
the Minister of Justice and Security and the State Secretary for Economic Affairs and Climate Policy:

4 Invest and cooperate in order to realise a secure universal and open digital eID system for an open, safe and prosperous society.

The State Secretary for Economic Affairs and Climate Policy:

5. Encourage the use of secure means of identification among citizens and businesses.

The Hague,

on behalf of the Cybersecurity Council,

Hans de Jong CSR co-chair	Pieter-Jaap Aalbersberg CSR co-chair