Making our services more personal

A series of projects have been launched aimed at expanding the SBR, for example a study involving sustainability reports. Via the innovation platform Digicampus we are also investigating ways to further update the SBR approach. Together with businesses, government organisations and the academic world, we are investigating the possibilities offered by new technologies, often in the form of experiments and scientific studies. SBR is for example the subject of one of the challenges in the Start-up in Residence programme.

The Dutch government (national government, provinces, municipalities and water authorities) are now all able to receive and process e-invoices. As a result, suppliers now have the right to send e-invoices, while the receiving and processing of e-invoices has become a requirement for government organisations. National government has in fact converted the right into an obligation for e-invoices, so today only one channel remains for receiving invoices, namely in the form of electronic invoices suitable for automated processing.

Within the Dutch government, we have undertaken to comply with the open standards for e-invoicing introduced by the market. This means that via his or her own software package, every entrepreneur can send an e-invoice direct to national government, municipalities, provinces and water authorities. The government's own e-invoicing helpdesk is available to answer any questions about e-invoicing. In 2019, this centre of expertise answered more than 14,000 questions from entrepreneurs.

Standardisation

The use of standards is a valuable tool in encouraging supplier independence, market forces and a secure and accessible digital government. The consequences of the corona crisis further emphasises the importance of digital access. The security of the links to government websites, email and applications must be in perfect order to prevent the misuse of government domains for phishing attacks and to ensure that the exchanged data and/or mail traffic cannot be intercepted or manipulated. The use of standards for information security, as laid down in the 'comply or explain' list, helps make this possible. Every year, the Dutch Standardisation Forum monitors the adoption of open standards. The Open Standards monitor for 2019 for example reveals a rise in the requests for open standards in tendering procedures. In 2019, one or more relevant standards from the 'comply or explain' list was requested in 89 percent of all tendering procedures (as compared with 85 percent in 2018).

At the same time, the survey reveals that there is still room for improvement when it comes to using open standards. For example, all relevant open standards were only requested in 6 percent of the investigated tendering procedures.

The most recent six-monthly information security survey by the Standardisation Forum also reveals that the level of application of the majority of information security standards has risen to well above 90 percent. The main area in which further improvement is needed is to prevent the misuse of emails from government domain names. The Digital Government Act includes a principle which, as the final stage in all policy-based interventions, offers the possibility for introducing compulsory standards. Among others, this applies to the information security standards HTTPS and HSTS (see the next section on 'Improving information security').

The Cabinet response dated 15 December 2019 to the report 'Inventory of Standardisation' also announced a series of actions relating to standardisation. These include focusing attention on the importance of open standards among procurement officers and contract-awarding parties by sharing knowledge with the various target groups. In particular, the spotlight was placed on the 'Open Standards Decision Tree' developed by the Standardisation Forum. This decision tree helps procurement officers and contract-awarding parties determine which standards are relevant for ICT orders by working through a series of questions. The Standardisation Forum has investigated how consultations about standards can be made known to a wider audience. An initial trial via internetconsultatie.nl has delivered promising results. The aim in the future is to publish consultations about open standards via this website.

Improving information security

Government Information Security Baseline

The Government Information Security Baseline (BIO) has been the basic standard framework for all levels of government since the start of 2019 (national government, provinces, municipalities and water authorities). The BIO is a joint product of all government organisations, and has immediate consequences for the protection of information provision by

municipalities, provinces, national government and the water authorities. To support organisations at all levels of government in implementing the BIO, a two-year programme has been developed (2019 and 2020).

Government procurement policy

It is vital that ICT products and services are digitally secure. In 2018, in conjunction with public and private parties, the Cabinet prepared the Digitally Secure Hardware and Software roadmap (roadmap DVHS). This roadmap is part of the Dutch Cyber Security Agenda (NCSA). One of the action spearheads in the DVHS roadmap is entitled 'Government Procurement Policy'. This action line will be developed on an intergovernmental basis as an integral part of NL DIGIbeter. Via its procurement policy, government can encourage the demand for digitally secure ICT products and services by including cybersecurity requirements in that procurement policy.

A first draft version of a manual and a *wizard* for Government Cybersecurity Procurement Requirements (ICO) was completed in 2019. The wizard makes it possible to select packages of requirements that specifically match the products and services to be purchased. During the first half of 2020, further experience of using this wizard will be acquired, in the form of a series of trials.

Compulsory use of HTTPS and HSTS

The consultation programme for the draft decree 'Decree on secure links with government websites and web applications' has now been concluded. The aim of this proposed decree is to make use of the information security standards HTTPS and HSTS compulsory for public access websites and web applications from administrative bodies. To encourage adoption of these safety standards, in addition to the regular monitoring by the Standardisation Forum, additional attention will be focused in 2020 on the provision of information to parties recognised as lagging behind. This 'catch-up process' will be undertaken among others via the channels operated by BZK and the Standardisation Forum.

System of national coverage

It is vital that government be thoroughly prepared for cybersecurity incidents. Against that background, intergovernmental agreements are currently being elaborated on preparations for digital incidents and cooperation in the event of digital incidents. Intergovernmental cooperation can increase the digital resilience of government. For this reason, a system of national coverage (LDS) has been included as an integral part of the NCSA.

The government is a participant and founding member of a Computer Emergency Response Team (CERT) and is helping to combine CERT with the National Cyber Security Centre (NCSC). The Security of Network and Information Systems Act (Wbni) of the Ministry of Justice and Security makes it possible to share information (including personal data and confidential derivable information) about threats, incidents and vulnerabilities. As a result, CERT is even better able to fulfil its vital role as an information hub in the system of national coverage. A number of security bodies from local levels of government have now also joined CERT, including the VNG's own information security service. This helps to further improve national coverage of digital incidents.

Exercises with cybersecurity incidents

The first Government-wide Cyber Exercise was organised in October 2019, bringing together 600 administrators, managers and professionals from national government, provinces, municipalities and water authorities, to practise dealing a cyber incident, that was made a true to life as possible.

Local disruption

As outlined in the Cabinet response to the report 'Preparing for digital disruption' published by the Netherlands Scientific Council for Government Policy (WRR), careful preparation for incidents must be made a vital element of our national security policy. Total prevention of digital incidents is not possible. At the same time, due to mutual interdependencies and the complexity and diversity of network and information systems, digital incidents can quickly result in large-scale and even cross-border effects. In collaboration with private organisations, government must therefore be prepared for incidents in the digital space.

To prevent local disruption, it is of key importance to secure the interplay that is necessary for preparing for digital incidents, and in tackling digital incidents whenever they do occur. One aspect of guaranteeing this interplay is reaching clear agreements with all government organisations that do not operate as part of national government, including municipalities, security regions, water authorities and provinces.

At municipal level, work is underway on a Municipal Digital Security Agenda. This agenda deals both with the security of the municipal organisations themselves, and administrative responsibility in the event of locally occurring cyber incidents.

Actions 2020-2021

- Each year, we investigate the experiences of citizens and entrepreneurs with government services. Government and Entrepreneurs

Standardisation

- Via internetconsultatie.nl, we involve a wide target group in the creation of standards.
- The Secure Link Decree has been through its consultation phase and will come into force as soon as the Digital Government Act has been approved by the Senate.
- We are focusing attention on open standards for procurement officers and contract-awarding parties. The Decision Tree developed by the Standardisation Forum helps clarify for them which standards are relevant to ICT orders.

Government and Entrepreneurs

- The focus in 2020 is on the rapid and simple access to online information about services from European governments. We are optimising customer journeys from the perspective of European cross-border life events. Individual citizens can find information about their life event at overheid.nl and government.nl, while the access points for entrepreneurs are ondernemersplein.kvk.nl and business.gov.nl
- In the cross-border and domain-overarching chain of data interchange, we are seeking to achieve further harmonisation between all stakeholders. Examples include SBR and e-invoicing. Public and private parties involved in the SBR have for example drawn up a joint roadmap for the next five years.
- We are constantly improving the Standard Business Reporting (SBR) approach, to further facilitate the reliable electronic interchange of data. This is above all achieved by experimenting with new technologies within the Digicampus, where government, the private sector and the academic world are collaborating closely. We are also investigating how SBR can contribute to the creation of reliable algorithms and data sharing.
- SBR is also part of the SiR programme. The aim is to map out a case with sustainability data to identify how reporting can be made easier and clearer for entrepreneurs, while the entrepreneurs maintain control of their own data.
- Together with private parties we are investigating how the SBR approach can be further expanded and how we can respond better to the new data economy. We are incorporating new technologies. We are also aiming to broaden the scope of e-invoicing, in particular or small and medium-sized enterprises.

Improving information security

- Once again in 2020, a cyber exercise will be organised but on this occasion it will be an entirely digital event. A series of webinars will be held in October, concluding with a virtual cyber exercise on 26 October. This programme will tie in with the annual campaign Alert Online and the European month of cyber security. During the webinars and the virtual cyber exercise, the focus will be on knowledge sharing and a consideration of the risks and the lessons learned from the huge rise in home working during the corona crisis. There will also be attention for the response of governments to the Citrix incident and other cyber incidents that have affected or could affect government organisations.
- In 2020, we will ensure that the Government Information Security Baseline (BIO) is implemented by more government bodies. In response to the corona crisis, the activities of the support programme will be adapted more quickly in virtual activities in the form of online courses and webinars. The accompanying products will be made available in digital format, wherever possible.
- The Uniform Standards Single Information Audit (ENSIA) will help to increase the level of adoption of the BIO and individual central systems, within municipalities. ENSIA will also assist in placing and keeping the subject of information security on the agendas of administrators and management, and will encourage talks about information security between the leaders and members of municipal councils. Another objective of ENSIA is at the same time to reduce the responsibility burdens (for municipalities). The instrument that supports the ENSIA system is currently being replaced. A European tendering procedure has already been initiated, the aim of which is to have a new instrument ready for deployment during the accounting year 2021. Parallel to the replacement of the instrument, work is also being carried out on improving the governance of the ENSIA system itself. The

evaluation is currently underway, and BZK will join the VNG and the system holders in improving cooperation, based on the outcomes.

- During the first half of 2020, in a series of trials, we will acquire experience with the Government Cybersecurity Procurement Requirements wizard, the aim of which is to ensure that suppliers of hardware and software satisfy the procurement requirements of government.
- With regard to the System of National Coverage (LDS), agreements have been reached on a Computer Emergency Response Team (CERT) and the links between the CERT team and the National Cyber Security Centre for the Information Security Service of Municipalities (IBD) and the Water Management CERT team operated by the water authorities. This year, the provinces will examine how they can organise their information hub.
- In 2020, a start will be made on investigating the frameworks and agreements required in response to local disruption caused by digital incidents. This will be carried out by municipalities, provinces and water authorities, together with the NCTV.
- Studies are being carried out into the legal basis for information security. In the next stage of the Digital Government Act, we will be examining whether and how generic information security should be given a permanent role. A start has already been made by drawing up an Integrated Consideration Framework (IAK). The IAK is part of the legislative process and for example includes issues relating to proportionality and supervision.