Connectis

Public guideline for the KvK (Chamber of Commerce)

This public guideline describes the applicability of the Chamber of Commerce registration number, including instructions on which processes are required for usage. Furthermore, a threat analysis provides information about the (security) risks that need to be managed during this process of using the Chamber of Commerce number for the purpose of eIDAS.

Usage of KvK

The Kamer van Koophandel (Chamber of Commerce) in the Netherlands issues a 'KvK-nummer' (Chamber of Commerce registration number) to organizations that have been registered in the national 'Handelsregister' (Business Register). The KvK-nummer is provided together with a 'vestigingsnummer' (branch number). The combination of the KvK-nummer and vestigingsnummer is unique and can be related back to a single organization. This non-transferrable number is used by the Dutch public sector in their interactions with businesses.

Public services even require this number in order for an individual to request a service for the organization they work for. An individual needs to proof that he/she is authorized to act on behalf of the organization. This includes business owners, the board and other employees that have been given the mandate to act on behalf of the business. Depending on the business form (e.g. VOF, and B.V.) different rules may apply. For more information, please contact the Dutch Chamber of Commerce.

These individuals are referred to as 'authorized signatories' or 'legal representatives'. An overview of the authorized signatories for each organization is listed in the national Handelsregister. European citizens can be added as an authorized signatory as well. This enables them to use their European electronic identification method to request a service as representative for the Dutch business they work for. Organizations can change the information in the Handelsregister at any time by contacting the Dutch Chamber of Commerce.

Access to the Handelsregister

It is common practice in the Netherlands to deliver an extract upon requesting services from the public sector and the private sector. Businesses can purchase a digitally certified extract from the Handelsregister at any time by contacting the Dutch Chamber of Commerce. Additionally, the Chamber of Commerce has introduced three (paid) tools:

1. API Search
2. API Profile
3. HR Dataservice

The API Search pulls up basic information about businesses based on several search criteria. The API Profile pulls up extensive information about a specific registered business. The API tools can be accessed by citizens, businesses and public administrations. The HR Dataservice enables a direct connection to the

Handelsregister. The most actual information be accessed in real-time and the information is sent in xml to the application. This tool is the only automatised connection. This system can be accessed by businesses and public administrations. Unfortunately, the tools offered by the Dutch Chamber of Commerce do not allow for automatic mapping to the overview of all the authorized signatories registered to an organization.

Mapping eIDAS attributes to KvK

Each European citizen whose electronic identification method is accepted by the 81 Dutch participating municipalities, automatically sends along set of attributes to the Dutch municipality through the Connectis Broker. The attributes that are delivered in the set are determined by each European country. Some of the data sets are in STORK 2.0 format, some are in eIDAS format and some are in a non-standard format. Some attributes are listed as mandatory, while others are optional. More information about this is provided in the Simplified eID Profile.

Due to the differences in data sets provided, mapping to the Chamber of Commerce is performed by using the common and mandatory attributes 'date of birth', 'name' and 'family name'. These three attributes make up the minimum set of attributes needed to map an individual to a legal representative in the Handelsregister. These attributes are also saved by the Dutch Chamber of Commerce the moment an individual is registered as a legal representative.

Unfortunately, the tools offered by the Dutch Chamber of Commerce do not allow for automatic mapping to the overview of all the authorized signatories registered to a business. Therefore, Connectis was forced to incorporate additional means of verification. This process is used for eHerkenning, a Dutch eID scheme for organizations, as well. For this eID scheme the process is certified. An official extract from the Handelsregister, issued by the Dutch Chamber of Commerce, is used for verification purposes.

Verification of KvK flows

From a user perspective, the process to map an individual to the legal representatives using additional means of verification, can be described as follows:

Situation	A user wants to access a service that requires a KvK number of the Dutch company for which the user is authorized to make a transaction. Hence, the user is listed as an authorized signatory or a legal representative. The user sends a digitally certified KvK extract (not older than 5 days) with proof of this status to Connectis.
Actor(s)	• Connectis Support Employee (Main): handles KvK verification request
Preconditions	• A request to verify a KvK registration has been made and is available in the Verification & Approval Tool by Connectis • The request to verify a KvK registration consists of all needed data to perform verification (KvK number, KvK extract, Name of requestor)
Postconditions	• The Connectis Support Employee has verified the KvK registration

	• The outcome of the verification is stored and shared with the requestor		
Main Course	**Step**	**Connectis Support Employee**	**Alternative**
	1	Opens a pending KvK verification request	
	2	Compares name of requestor with name on KvK extract and KvK number and verifies the authenticity of the KvK extract	
	3	Registers outcome of verification and informs requestor	

Future expectations KvK

Connectis would like to automatically map individuals to a legal representative for a Dutch organization. The Dutch Chamber of Commerce would need to develop a new product to enable this. The pilot 'Bevoegdheidscheck' (Authorization check') could change the playing field. Participants to this pilot are developing a system which allows them to check, in real-time, whether an individual is a legal representative of the business they represent.

The focus of the pilot is for requests for the Dutch electronic identification method eHerkenning (eRecognition). However, once the technical solutions works in a test setting and in production, this tool could be easily used for the requirements of eIDAS. While the Chamber of Commerce does not currently offer the option to participate in the pilot, Connectis has expressed interest in the development of the Bevoegdheidscheck to an in-production product.

Connectis

Threat analysis

Security vulnerabilities have been identified in the aforementioned process. These vulnerabilities are identified as possible threats to the functionality of the process:

- Manual verification: the KvK procedure relies on a support employee at Connectis checking the information. There is a risk of human error involved, despite of the security measures[1] that have been undertaken.
- No real-time verification: the user uploads a KvK extract that is not older than 5 days. However, in those 5 days, the user may no longer be listed as a legal representative. As there is is no automatic real-time tool available currently, there is a risk that the user requesting services is not authorized to do so.
- Cross-Site Scripting (XSS) vulnerabilities: A3 of the Top 10 security vulnerabilities of OWASP describes the possibilities for intentional harm with regards to cross-site scripting:
    - Malicious code[2]: The hacker enters malicious code in the un-sanitized pdf file. The support employee could become the victim. The pdf file with malicious code can also be shown and executed directly on the approval tool or at the municipality.
    - Brute-force attack: There is an extremely small threat of a brute-force attack. The user is given a secure link for re-directing. If the hacker hits the secure link on the right moment, the hacker can access the user input form. They can use this to upload malicious code using the un-sanitized pdf upload.
- Man in the Middle Attack: the user could be hacked and be forced to access a certain proxy. This proxy makes the user think he/she is on the right page. Once the secure link is sent to the proxy, this secure link is consumed by the proxy and the hacker can access the user input form. They can use this to upload malicious code using the un-sanitized pdf upload. Furthermore, the 'man in the middle' attack allows the hacker to redirect the user to any webpage. This attack could also be done over an https connecting, despite of the usage of SSL encryption between the user and the server.
- Alternative Man in the Middle Attack: instead of the hacker going to the form, the hacker waits for the user to access the secure link. The hacker waits for the user to upload the pdf, when the hacker Intercepts the extract. This extract contains sensitive information (KvK information in the case of a KvK extract).
- Minimal set of attributes: only the attributes date of birth, name and family name are used to verify the user. This opens up the risk of misinterpretation. People with the same name could access the public services without being authorized.

[1] Connectis requires all employees to be in the possession of a 'Verklaring Omtrent Gedrag' (Proof of Goo Conduct - 'VOG'). Furthermore, the tool can only be accessed by authorized users.

[2] This vulnerability is safeguarded by the installation of a pdf sanitizer tool to remove code. This will be implemented early 2017.