Connectis

Public guideline for the Register Niet-Ingezetenen

This public guideline describes the Register for Niet-Ingezetenen, 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 Register for Niet-Ingezetenen for the purpose of eIDAS.

Usage of BSN

The Netherlands issues a 'burgerservicenummer' (citizen service number also know as 'BSN') for registered citizens. The BSN number is unique and can be related back to a specific individual. This non-transferrable number is used by the Dutch public sector in their interactions with citizens. Many services even require this number in order for the individual to proceed.

The usage of the BSN number is under strict supervision. The legislation that discusses the requirements for the BSN number is 'Wet algemene bepalingen burgerservicenummer'. Aside from the public sector, organizations are not allowed to request the BSN number from an individual, unless they have legal permission to do. An example of this is usage by the national healthcare sector. Organizations with permission to request BSN numbers also have access to the register that includes all BSN numbers of Dutch citizens. They need this to verify whether the BSN number provided by the individual matches the personal data that has been provided. Hence, the BSN number can be used to proof whether an individual is who they say they are.

Usage of RNI

The BSN number is only used in the Netherlands. Therefore, new citizens and non-residents need to request this number. Also Dutch citizens who have moved abroad before the 1st of October 1994 do not have a BSN number. New citizens that expect to spend at least four months in the Netherlands are obliged to register to the 'Basisregistratie Personen' (Basic Registration for Persons - 'BRP'). By doing so, they receive a BSN number. For non-residents that expect to spend less than four months in the Netherlands or former Dutch citizens who moved abroad before the 1st of October 1994, the 'Register Niet-Ingezetenen' (Register Non-Residents - RNI) has been designed. 19 Dutch municipalities[1] allow non-residents to register in order to receive a BSN number. Individuals need to bring valid proof of identification and they need to provide the address on which they are registered abroad. The result of this registration is an extract with the BSN number. This extract is used by Connectis for mapping purposes.

Mapping eIDAS attributes to RNI

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

[1] Alkmaar, Almelo, Amsterdam, Breda, Den Haag, Doetinchem, Eindhoven, Goes, Groningen, Heerlen, Leeuwarden, Leiden, Nijmegen, Rotterdam, Terneuzen, Utrecht, Venlo, Westland, Zwolle

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 Register for Non-Residents (RNI) is performed by using the common and mandatory attributes 'date of birth', 'name' and 'family name'.

Dutch municipalities have access to the Register for Non-Residents and can use the attributes provided by the Connectis Broker to verify the user. Connectis, on the other hand, is not allowed to access this system due to Dutch legislation described under section 'Usage of BSN'. Therefore, a procedure has been designed for the Dutch municipality who opens up one BSN-required service. Using the software developed, they are able to verify the user's identity. This municipality has also signed a 'Bewerkersovereenkomst' (Data Processing Agreement) with Connectis. This agreement describes the criteria under which Connectis is allowed to store the BSN numbers of users for the purpose of enabling this service.

Verification of RNI flows

From a user perspective, the process to verify a RNI registration can be described as follows:

Situation	A user wants to access a service that requires a BSN number obtained from the RNI. The user uploads the extract that was provided upon successful registration to the RNI to a server of Connectis.			
Actor(s)	• Connectis Support Employee (Main): handles RNI verification request • Municipality Employee (Secondary): verifies a RNI registration			
Preconditions	• A request to verify an RNI registration has been made and is available in the Verification & Approval Tool by Connectis • The request to verify an RNI registration consists of all needed data to perform verification (e.g. RNI number, RNI extract, Name and date of birth of requestor) • There is a 'Bewerkersovereenkomst' in place			
Postconditions	• The Municipality Employee has provided the outcome of the verification • The outcome of the verification is stored and shared with the requestor			
Main Course	**Step**	**Connectis Support Employee**	**Municipality Employee**	**Alternative**
	1	Opens a pending RNI verification request and downloads the attached RNI extract		
	2	ZIPs the RNI extract and protects it with a password. Mails the RNI extract compressed to a ZIP archive to a designated employee of the		

		municipality (note: the password to open the RNI extract **is not to be included** in the email)		
	3	Calls the designated employee at the municipality		
	4	Informs there is a request to verify an RNI registration and shares password		
	5		Opens email and unzips the RNI extract with the provided password	A2: cannot unzip with password
	6		Verifies the RNI extract with the BRP register and the personal data provided by the user	
	7		Replies to Connectis Support Employee during phone call	
	8	Registers outcome of verification and informs requestor		

In case the extract can not be unzipped with the password, the following alternate course comes into place:

Alternate Courses	**Step**	**Connectis Support Employee**	**Municipality Employee**	**Alternative**
	A1.1		Notifies zip file cannot be opened with provided password	
	A1.2	Continues with step 2 of the main scenario		

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 RNI procedure relies on a single employee at the municipality who is authorized to grant access for users using the BRP register to confirm their RNI extract. While Connectis has requested the municipality to provide us with the direct contact information, there is a risk of the user answering the phone at the municipality is not who they say they are. The person who answers the phone and indicates that he/she is allowed to make the decision, might in fact not be the person who is granted authority to do so. This allows for human error or intentional harm.
- 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. Connectis is implementing a pdf-sanitizer to remove all Javascript to solve this risk.
    - 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 (BSN number in the case of RNI process)

Furthermore, there is a strong dependency on the BRP register, to which Connectis does not have access. The RNI extract does not allow for real-ti9me verification. This means that the BRP register is always needed to verify the user.

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