SKG-IKOB AE 3104
17-04-2024

SKG-IKOB
Certificatie

bezoekadres
Poppenbouwing 56
4191 NZ Geldermalsen

postadres
Postbus 202
4190 CE Geldermalsen

T +31 (0)88 244 01 00
F +31 (0)88 244 01 01
E info@skgikob.nl
I www.skgikob.nl

ADDITIONAL REQUIREMENTS

FOR THE ISSUE OF A KOMO® APPROVAL-WITH-PRODUCT CERTIFICATE FOR SECURITY PRODUCTS FOR WINDOWS AND DOORS BASED ON BRL 3104

Established by the Board of Experts for Safe and Burglar Resistant Products
date 8 April 2024

GENERAL INFORMATION

At its meeting on 17-04-2023, the Board of Experts for Safe and Burglar Resistant Products (CvD-V&I) decided that BRL 3104 is the basis for product certification of security products for windows and doors.
This BRL refers to classification and testing methods according to NEN 5089 and to this SKG-IKOB AE.
The CvD-V&I formed the support committee for drawing up this document.

Decisions made by the Board of Experts will be added to this document where relevant and interested parties will be informed in an appropriate manner.
For the most recent version of this document, the SKG-IKOB website should always be consulted.

The following parties are represented in the CvD-V&I:

- BouwendNederland (department glass)
- VHS (association of manufacturers of building hardware)
- FVN (Dutch Federation for security)
- National Police (NP)
- CCV – PKVW (Centre for Crime Prevention and Security)
- VvV (Insurance association)
- SKH (Certification institute for wood products)
- NSSG (Dutch Guild of locksmiths)
- NL-Ingenieurs (Dutch association of engineering consultants and civil engineers)

SKG-IKOB Certificatie BV
Poppenbouwing 56
Postbus 202
4190 CE Geldermalsen
T: +31 (0)88 244 01 00
F: +31 (0)88 244 01 01
E: info@skgikob.nl
I: www.skgikob.nl

INTRODUCTION

The national assessment guideline BRL 3104 is the certification basis for burglar-resistant building hardware (the granting of SKG stars) and refers for the requirements and test methods to;

NEN 5089 - Burglar resistant building hardware - Requirements and test methods.

This NEN national standard does not cover all conceivable security products for windows and doors and by its nature a relatively static document.
For this reason, assessment guideline BRL 3104 refers not only to NEN 5089 but also to this document;

SKG-IKOB AE 3104 - additional requirements

This incorporates the decisions made by the Board of Experts as additions or alternatives to NEN 5089. These also form the basis for SKG-IKOB certification of security products.

NO	DESCRIPTION	PAGE

01 Alternative product requirements for manual tests 5
02 Additional product requirements for electromechanical and electronic building hardware 6
03 Product requirements for seam protectors on doors (lock side) 18
04 Marking conditions for emergency and panic devices 19
05 Alternative provisions for durability & corrosion resistance of locks 20
06 Further explanation & criteria for manual testing 21
07 Product requirements for code locks 23
08 Product requirements for mechatronic padlocks 25

Annexes:

Model self-declaration 26
Wood*) 3 minutes (2-star) 33
Wood*) 5 minutes (3-star) 39
PVC 3 minutes (2-star) 45
PVC 5 minutes (3-star) 48
Aluminium 3 minutes (2-star) 50
Aluminium 5 minutes (3-star) 52

**) Profile details as well as hanging- and closing seams must be executed in accordance with the KVT, edition; Dutch Industry Association for the Timber Industry (NBvT)*

01 Alternative product requirements for manual tests

CvD decision: 15-08-05 / 16-03-11 / 06-09-12 / 16-12-16 / 12-7-17

Introduction

Many years of experience at SKG-IKOB have shown which values for the strength and dimensions of certain products are sufficient to assume that they will be eligible for categorisation in a class as described by NEN 5089. These criteria can then replace the manual testing for this specific product range.

Decision

For the following products laboratory tests are an alternative to manual testing***)**.

***)** *If these laboratory values are not satisfied, this does not mean that the product is not burglar resistant. Burglar resistance must then be demonstrated by means of a manual test!*

Product / Test	**Classification**		
Main lock, side lock or latch with straight bolt (block or pin)	**1-star**	**2-star**	**3-star**
Bolt length	≥ 20 mm		
Side load(s) on bolt (unsupported; distance 6 mm)	4 kN	6 kN	
End load on bolt (with well fitted locking box)	2 kN		
Keeper for locks or latches with straight bolt (block or pin)	**1-star**	**2-star**	**3-star**
Side load on locking edge (pressure piece, depth 14 mm, width = bolt width)	4 kN	6 kN	
End load on backside box	4 kN		
Slide door lock	**1-star**	**2-star**	**3-star**
Resistance lock mechanism (torque)		≥ 95 Nm	
Burglar resistant hardware, if from solid metal strip (alu., brass or steel)	**1-ster**	**2-ster**	**3-ster**
Shields without extraction protection: push test in accordance EN 1906:A3.3 - 30.18; permanent deformation ≤ shield thickness - 4 mm, parts may not collapse		10 kN	15 kN
Shields with extraction protection: push test in accordance with EN 1906:A3.3 - 30.20; permanent deformation ≤ shield thickness - 4 mm, parts may not collapse		15 kN	
Tensile test in accordance with EN 1906:A3.4 - 30.19; permanent deformation ≤ 5 mm, parts may not collapse		15 kN	20 kN
Resistance of handle pin for lift and slide door hardware (torque)		≥ 65 - ≤ 85 Nm	
Hinges with burglar-resistant pin/cam	**1-star**	**2-star**	**3-star**
Pin/cam length		≥ 18 mm	
Side load on pin (hinge plate distance + 6 mm); deformation of pin ≤ 8 mm		6 kN	7 kN
Garage door operator	**1-star**	**2-star**	**3-star**
Fixing / mounting points cannot be released / reached manually (NEN 5096)		judgement	

02 Additional product requirements for electromechanical and electronic building hardware

CvD decision: 17-04-23 / 08-04-24

1 Introduction

A growing number of products intended for locking and unlocking windows and doors are fitted with electromechanical and/or electronic components. Since the regular standards, in accordance with SKG-IKOB BRL3104, are insufficiently tailored to these products, SKG-IKOB, in close collaboration with interested market parties, has compiled additional requirements in this document.

SKG-IKOB only assesses the products for durability and burglar-resistant properties. The other***)*** standards and regulations that a product, or the solution that the product is part of, may have to comply with are not tested or assessed by SKG-IKOB.

) *Other standards and regulations include the AVG and CE and all related directives.*

2 Subdivision of products

The following categories can be defined for products:

- **Mechanical products;** this category includes:
  products that only operate mechanically and do not use electromechanical and/or electronic components for any functionality in relation to actual locking or unlocking.

  These additional requirements do not apply to the 'Mechanical products' category.

  Remark: Products fitted with window/door position and/or handle position and/or latch position sensors solely for signalling purposes are also included in this category.

- **Electromechanical products;** this category includes:
  Products fitted with one or more electromechanical and/or electronic component(s) which, collectively or otherwise (among other things), have the purpose and/or (secondary) effect of being able to unlock and/or lock the product via an electrical signal, usually in the form of the application or removal of a supply voltage.

  Explanation: This category includes most electric locks and strike plates.

- **Electronic products;** this category includes:
  Products that are equipped with one or more electromechanical and/or electronic components which, collectively or not (among other things), have the purpose and/or (secondary) effect of being able to unlock and/or lock the product via an electrical signal, other than the power supply voltage, or a wireless signal.

  Explanation: This category includes all locks which (among other things) have the purpose and/or (secondary) effect of enabling the lock to be unlocked and/or locked via an electronic or wireless signal, including but not limited to signals transmitted via radio waves (RF), light signals such as infrared light (IR), audible or inaudible sound signals or mechanical vibrations (including knocking and tapping).

3 Scope

These additional requirements apply to all products in the categories: 'Electromechanical products' and 'Electronic products'. It describes the requirements for the systems for distribution, storage and processing of digital keys***)*** for authorisation of operation and/or (de)activation of locking.

Basically, products from the categories: 'Electromechanical products' and 'Electronic products' should primarily comply with the requirements as defined in NEN 5089.

) *Where the term 'key(s)' is used in this document, a key means: any form of code (carrier) with which the product can be operated. Internationally, this is often referred to as 'credential(s)'.*

3.1 Basic System Model

These supplementary requirements (AE) consider each product or composition of products offered for assessment as a system, for which the basic system model is given on the next page. Each product or composition of products can be reduced to the basic system model. In this respect, an electronic lock with a key management environment may fulfil all components of the system model and the make-up for an electromechanical lock may be limited to one component and one link (Link D and Actuator).

This AE sets requirements for each component and each link within the basic system model.

In the event of contradictions between this AE and other applicable legal standards or regulations, this must be reported to SKG-IKOB and this AE will be adjusted by SKG-IKOB. In the event of contradictions with other applied (non-statutory) standards or private requirements, this will be raised with the Board of Experts and discussed.

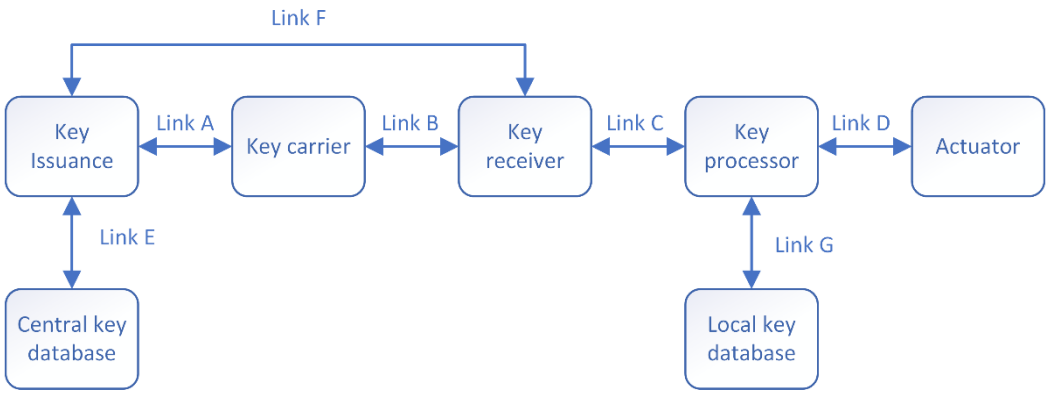


Figure 1: Basic system model

Explanation: *'Basic System Model'*
The basic system model consists of functional components, which in practice are not always separate parts. The requirements relate to the functional components and therefore form the total requirements for the physical product or composition of products.

The basic system model consists of the following components:

- 'Key Issuance' includes all systems, components and processes that, by any means, produce or generate keys for the system. This includes, but is not limited to, management applications, online management environments, production of RFID transponders, production of remote controls, etc.
- 'Central key database' includes all systems, components and processes that, by any means, store more than a single key produced or the keys to be produced, other than the 'Key carrier' and the 'Local key database'.
- 'Key carrier' includes all systems, products or components which are used, by whatever means, to transfer the key from the 'Key issuance' to the 'Key recipient'. This includes, but is not limited to, RFID transponders, remote controls, QR codes, etc.
- 'Key Receiver' includes all systems and components that, by any means, receive or read keys. This includes, but is not limited to, RFID readers, remote control receivers, QR code readers, PIN code input devices, etc.
  The key receiver controls communication with the key carrier and/or key issuance and transfers the received key to the key processor.

  Explanation: *'Key receiver'*
  If the 'Key Receiver' is physically divided into an antenna and electronics that process the antenna signal, then the connection between the antenna and the other electronics should be considered an extension of 'Link B' and should meet the same requirements. as 'Link B'
- 'Key Processor' includes all systems and components that, by any means, control and process the key received by the 'Key Receiver'. If a 'Local Key Database' is present, the 'Key Processor' may compare the offered key with the keys in 'Local Key Database'. and determine whether or not the presented key allows access.
- 'Local key database' includes all systems, components and processes where and through which, by whatever means, the keys accessed at the electronic lock are stored within the relevant electronic lock.
- 'Actuator' means that part of the electronic lock which converts the electronic approval of the 'Key Operator' into a mechanical action.
- 'Link A' to 'Link G' constitute the internal or external connections, by whatever means, between the various components. This includes, but is not limited to, internal connections on a PCB (Printed Circuit Board), wireless radio connections, connections over the Internet, etc.

4 Classification

On the one hand, the current state of technology no longer impedes the creation of secure electronic locks in any way; on the other hand, the current state of technology makes it increasingly easy for malicious parties to manipulate or bypass security techniques. This is why all products, regardless of whether they are certified for SKG 2- or 3-star, must meet these additional requirements.

As far as requirements are concerned, a distinction is made only between internal wired connections, including but not limited to those on the product's PCB (Printed Circuit Board), if any, which are within the 'secure zone'***)*** and all other connections.

) *'secure zone' and/or 'secured zone' refers to the area (zone), that cannot be accessed without breaking, if this area is closed off (locking in closed position) by means of the relevant (under inspection) product.*

5 Requirements

5.1 General

The requirements are defined for each component of the basic system model and set out in the following paragraphs. If a system component fulfils the function of several components, this system component must meet all the requirements for the individual components.

The manufacturer of the system must specify its product using the basic system model (Figure 1) and declare clearly and unambiguously that the requirements that apply to the product are met. For the self-declaration the 'Model self-declaration' must be used as included to the annex.

5.2 Products and product combinations

'Key carriers' and/or accessories and/or peripherals such as but not limited to 'Key receivers' that can be used in combination with the product and must be covered by the certificate to be obtained must be specified and be part of the response and self-declaration. In other words, the self-declaration must also be accurate for relevant components and products. These parts and products are an integral part of the certificate and as such are also mentioned on it. The manual must clearly state the combination of products that the SKG certificate is valid for and explicitly state that the SKG certificate is not valid for other combinations.

5.3 Requirements for signal transmission

The following requirements are set for signal transmission within each link (Link A … Link G):

Type of link (accessibility)	Example	Cryptographic encryption	Length of cryptographic key	Validity of cryptographic key	Protection against accepting a copied message	Authentication**	Integrity check***
Internal, contact Product in secure zone	including internal wiring in the product, also PCB	Not necessary	n/a	n/a	n/a	n/a	n/a
Internal, contact Product in unsecured zone	including internal wiring in the product, also PCB	Yes, AES128* or better	≥128 bits	Infinite	Yes	Yes	Yes
External, contact, secure zone	including wiring outside the product, applied in the secure zone.	Not necessary	n/a	n/a	n/a	n/a	n/a
External, contact, unsecured zone	including wiring outside the product, applied in the unsecured zone.	Yes, AES128* or better	≥128 bits	Infinite	Yes	Yes	Yes
Wireless, regardless of the technology used or distance to be covered and regardless of the security zone in which the product is installed.	RFID transponders, wireless remote controls, Bluetooth, Wi-Fi, Zigbee, Z-wave, light signals, sound signals, etc.	Yes, AES128* or better	≥128 bits	Infinite	Yes	Yes	Yes
Public networks	including internet connections.	Connection security is determined by the server the connection is made to. This server should have at least an **A+** rating, testing via: https://www.ssllabs.com/ssltest/index.html					

Table 1: Requirements for each link

* *AES128 or a demonstrably equivalent or better open-source alternative, including the reference to the open source.*
** *Authentication is the process of verifying that a user (can also be a device or part thereof) is actually who they claim to be.*
*** *Integrity check: checking the integrity of the data.*

5.4 Requirements for access to and storage of key data

Requirements for access and storage of key data include encryption, authentication and integrity checking.

In general, all identification data, such as key information, user data and passwords, must be unreadable between:

- ‘Key issuance’ and the ‘Local key database’
- ‘Key issuance’ and the ‘Central key database’

In addition, access to key data must be authorised and authenticated.

To achieve this, all identification data within the relevant components must be encrypted. Tabel 2 provides an overview of the requirements:

Component	Cryptographic encryption	Authentication[7]	Authorisation[8]	Integrity check[9]
Key issuance	Yes, AES128[1] or better	TFA or MFA[2] is mandatory if more than 10 own products or one or more third-party products can be managed (see explanation). For all other situations, it may be possible to disable TFA or MFA[2] optionally, with a reduced security notification.	Login with unique username[4] and password[5].	Yes
Central key database	Yes, AES128[1] or better, unless the 'Central key database' is processed on the same server as the 'Key issuance' application and this server is housed in an ISO27001 certified data centre[6] and, in addition, the data is stored on an AES128[1] or better encrypted storage medium.	Yes, minimum MAC[3], unless the 'Central key database' is processed on the same server as the 'Key issuance' application and this server is housed in an ISO27001 certified data centre[6] and, in addition, the data is stored on an AES128[1] or better encrypted storage medium.	Login session, unless the Central key database is processed on the same server as the Key issuance application and this server is housed in an ISO27001 certified data centre[6].	Yes
Key carrier	Yes, AES128[1] or better, unless the 'Key Carrier' only transfers the key and does not store it itself and, moreover, the key in question can only be used once.	Yes, minimum MAC[3], unless the 'Key Carrier' only transfers the key and does not store it itself and, moreover, the key in question can only be used once.	Login session, unless it can be made plausible that the key (data) cannot be read in any way if an expert has unlimited access to the 'Key carrier'.	Yes
Key receiver	Yes, AES128[1] or better, unless the 'Key receiver' only transmits the key and does not store it itself and, moreover, the 'Key receiver' and 'Key processor' are part of the same product (housed in the same enclosure) and the product is located in the secure zone.	Yes, minimum MAC[3], unless the 'Key receiver' only transmits the key and does not store it itself and, moreover, the 'Key receiver' and 'Key processor' are part of the same product (housed in the same enclosure) and the product is located in the secure zone.	n/a	Yes
Key processor	Yes, AES128[1] or better, unless the 'Key processor' only processes the key and does not store it itself and, moreover, the 'Key receiver', 'Key processor' and local key database are part of the same product (housed in the same enclosure) and the product is located in the secure zone.	Yes, MAC[3] or better, unless the 'Key processor' only processes the key and does not store it itself and, moreover, the 'Key receiver', 'Key processor' and local key database are part of the same product (housed in the same enclosure) and the product is located in the secure zone.	n/a	Yes
Local key database	Yes, AES128[1] or better, unless the 'Local key database' and 'Key processor' are part of the same product (housed in the same enclosure) and that product is in the secure zone, or it can be argued that the key (data) cannot be read in any way via internal (within the housing of the product) or externally available interfaces if a person skilled in the art has unlimited access to the product with the 'Local key database'.	Yes, minimum MAC[3], unless the 'Local key database' and 'Key processor' are part of the same product (housed in the same enclosure) and the product is located in the secure zone.	n/a	Yes
Actuator	n/a	n/a	n/a	n/a

Table 2: Requirements for storing data within each component

(1) AES128 or a demonstrably equivalent open-source alternative, including the reference to the open source.
(2) TFA or MFA: Two-factor authentication or multi-factor authentication (see explanation below).
(3) MAC: Message authentication code.
(4) Username: unique identifier of a person (e.g. e-mail address, phone number or external authentication provider ID).
(5) Password: password, authentication code or authorisation from external authentication provider.
(6) Instead of 'ISO27001 certified data centre', the term 'a secure area at the user's location' may also be used, in which case the ISO27001 requirement is dropped. If the data centre is an in-house secure environment of the certificate holder, for example, it must still be ISO27001 certified.
(7) Authentication is the process of verifying that a user (can also be a device or part thereof) is actually who they claim to be.
(8) Authorization is the process of giving a user (can also be a device or part thereof) permission to use a certain resource or function.
(9) Integrity check: checking the integrity of the data.

Explanation: *'Table 2: Requirements for data storage within each component'*

I. TFA or MFA is mandatory if more than 10 own products are managed. In this context, own products are products that provide access to a living or accommodation area that is used by the manager himself.

II. TFA or MFA is mandatory if one or more third-party products can be managed. In this context, third-party products are products that provide access to a living or accommodation area that is not used by the manager himself.

III. If third-party services are used for authentication, such as Apple, Google, Facebook or Microsoft, this authentication method must also include TFA or MFA, unless a trust relationship that is equal or better can be guaranteed within the authentication method used. then TFA or MFA.

5.5 Requirements for storing passwords and keys

Passwords and PIN-codes (keys to be transferred by a person), may not be stored within the central database and may not be traceable. This means that a user or administrator, whatever their level, cannot retrieve or view this data in any way. It is of course permissible, for example, to store and compare a hash of this data.
The above also applies to the local database, if the local database is accessible via public networks.

5.6 Operating requirements

Locks or the products designed for them can be operated according to the following principles:

- ***Direct control***; where the basic system model is reduced to only an 'actuator', which is directly controlled by an electrical signal ('Link D').
- ***Local control***; where the person operating the lock is in direct proximity***)*** of the lock and operates the lock with the intent to pass the corresponding door itself.
- ***Remote operation***; where the lock is operated:
  - from a location not in proximity of the lock, or;
  - by a person who has no intention of passing through the door itself, or;
  - by another product or system, whether automated or not.

) *Direct proximity is defined as a distance approx. 25m, where the operator has a direct view (not by a camera) of the door and can control the closing status of the door.*

The system must allow users to unlock locks (unlocked) and lock the same locks (locked).

There are no additional requirements for operation according to the 'Direct control' and 'Local control' principles, other than the signal transmission requirements for example; RFID transponders or remote controls or other digital keys in any form.

5.6.1 Requirements for ‘Remote operation’

If a lock with 'Remote Operation' principle is applied, the door may only be unlocked***)*** temporarily (maximum 30 seconds).
The above applies unless:

- The user is made aware of the security aspects that ‘Remote operation’ could entail and;
- A change in the door position (door 'open' or 'closed') within 15 seconds after the change is passed on to the person or system who operated the lock and;
- A change in the latch position (bolt out is 'locked', bolt in is 'unlocked') of the deadbolt of the lock within 15 seconds after the change is passed on to the person or system operating the lock and;
- A clear indication of the door status*****)*** is displayed to the person or system operating the lock, with the door being marked as ‘locked’ only if the door position is ‘closed’ and the dead bolt position of the lock is ‘locked’.

) *Unlocked: the door cannot be opened or pushed open automatically without the need for an additional action, for example operating a handle.*

*****)*** *Door status: combination of door position and latch position. The door status is ‘locked’ only if the door position is ‘closed’ and the latch position of the lock’s dead bolt is ‘locked’.*

6 Software and firmware requirements

The following additional requirements are imposed on the software and firmware associated with the product or system:

- Software (apps) for phones, computers or other devices must be adequately updated if security problems have been identified in the existing software. In the event of an online service for the user, these updates must be provided automatically; in the event of software for telephones, computers or other devices, this software must be made available to the user so that it can be installed by the user themselves. You must state that and how this has been achieved for the product and associated management and access tools.
- The products’ firmware must be adequately updateable if security issues are identified within the existing firmware. It must be possible for these updates to be performed in the field by the user or in an automated manner. Hence, there must be no need to return the product to the supplier or manufacturer, for example, for this to be done. If security problems are identified in the existing firmware, new firmware, with the security problem fixed, must be made available to the user free of charge during the validity of the certificate.
- The product must be secured against accepting firmware that is not made and signed by the manufacturer via FOTA***)*** or USB, for example.

) *FOTA: Firmware over the air, i.e. the ability to update firmware via a wireless connection.*

Explanation: *'Requirements for software and firmware'*

I. When products are stand-alone, the above requirements continue to apply. Naturally, automatic updates will not be possible in that case. However, the user must be able to perform the update himself and the firmware must also be made available to the user free of charge.

II. When apps supplied or made available by the manufacturer are used for telephones, computers or other devices, the manufacturer no longer has to provide updates to that app for the relevant devices if these devices are no longer supported by their manufacturer or no longer (can) receive updates.

7 Requirements for digital keys

Additional requirements are imposed on digital keys, regardless of the carrier, as shown in paragraphs 7.1 and 7.2.

7.1 Keys to be entered or transferred by a person

Keys entered or transferred by a person, including but not limited to PIN-codes, are subject to the following requirements:

- They must have a minimum length of 4 digits or 4 characters.
- They must be unique within the system (the management environment for a specific lock). It must not be possible to assign the same PIN code or digital key to multiple users within the same management environment.
- They must be demonstrably linked to a person. Namely, the use of a PIN code, without the PIN code itself being named, must be logged and linked to the user to whom that PIN code is assigned.

7.2 Keys to be entered or transferred via technology

Keys that are entered or transferred via technology, including but not limited to RFID transponders, remote controls, QR codes, etc., are subject to the following additional requirements:

- They must have a minimum length of 20 bits or 1.000.000 code variations.
- The combination of the keys and the encryption used for them must be unique. This means that the keys cannot be used as valid keys in any other system without explicit permission.
- They must be stored encrypted, see also ‘Table 2: Requirements for storing data within each component’
- They must feature an authentication method, see also ‘Table 2: Requirements for storing data within each component’.

8 Requirements for electronic keypads

Electronic keypads may comprise of the following, inter alia: physical buttons, tactile or pressure-sensitive surfaces, tactile or pressure-sensitive displays.

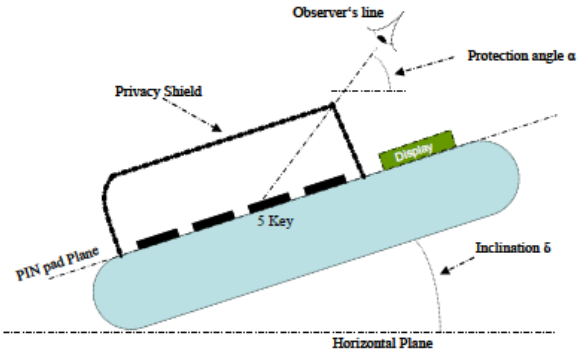
Due to the increased risks associated with the use of keypads and/or PIN codes, a product with a keypad can never be rated higher than SKG 2-star.

Electronic keypads intended for the entry of a digital key, e.g. in the form of a PIN code, must comply with the following requirements in addition to or to further clarify the requirements for the components in the basic system model:

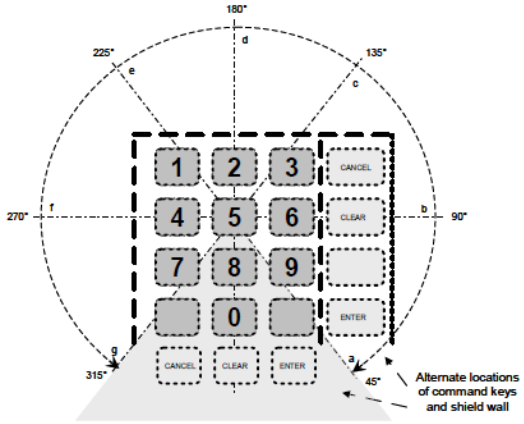
- The keypad (key receiver) must not be combined with the key processor and/or actuator, unless the assembly of key receiver, key processor and actuator are housed in one product (housing) and the entire product is located within the secure zone***)**.
- The keypad (key receiver) must have a security link with the key processor that prevents the keypad from being exchanged without requiring an update (logging in / linking up) from the key processor.
- The number of PINs that can be entered per hour must be limited so that the maximum number of PINs to be entered in a consecutive 48-hour period does not exceed: the maximum number of possible PINs divided by the reading speed, divided by the maximum number of users to which a PIN can be assigned, divided by 2. In this context, the reading speed is determined by the maximum number of codes that can be entered per hour.
- Keypads should be equipped with a shield that limits viewing, unless viewing from public areas is not possible due to the technology used for the keypad. If the shield is supplied as an optional component, this must be clearly stated in the instructions for use and the installation instructions. These must contain a clear warning of the risk of being monitored if no shield is used and explicitly state that if used without an approved shield the SKG certificate is not valid.
  If a keypad app is used on a personal mobile device, the above shielding requirement is not applicable.

- The shielding must comply with the requirements in EN 16867:2021 under ‘Protected visibility’:

  - The height of the shielding is determined by a radius from the reference point (the 5 key and/or the center of the code panel) at an angle ≥ 30 degrees from the protection zone.



Shielding height



Protection zone

***)** *'Safe zone' and/or 'secure zone' refers to the area (zone) that cannot be reached without being forced.*
If this area is closed (locking in closed position) using the relevant product (subject to inspection), this product must be able to withstand manual testing according to SKG 2-star.

8.1 Enabling and disabling PIN code functionality

If an SKG 3-star product has the option to enable a PIN-code, the product must meet the following requirements:

- The functionality that enables PIN-code entry must not be on by default.
- If the PIN-code entry functionality is implemented via a graphical or text-based user interface, a clear warning must be given, whereby it is explicitly stated that the SKG certificate is downgraded to SKG 2-star level when the function is enabled.
- If the PIN-code entry functionality is enabled via a jumper or switch, this should only be possible after a seal has been removed, which explicitly states that the SKG certificate is downgraded to SKG 2-star level when the function is enabled.

9 Biometric readers

If the key receiver within the basic system model is a biometric reader, this biometric reader must at least comply with ‘Grade C’ of the ‘credential-related security’ requirements as stated in EN 16867:2021:

- FAR^{-1} / max. number of auth. templates: 10.000
- Additional security features: alive detection

10 Other requirements

10.1 Requirements regarding the product

- The product and/or related apps and/or management applications in any form whatsoever must not contain any pre-programmed or traceable passwords, access codes, access keys or anything of that nature after installation or commissioning has been completed.
- Once the product has been installed and commissioned, it must not be possible for it to change ownership without the intervention of the owner or product manager. In this context, it must also not be possible to link the product to a management application or management platform more than once.
- Passwords for access to an online service for management and/or configuration of the product must at least meet the criteria set for the key issue component within the basic system model.
- The security of the product and associated data must be maintained if one or more components of the overall solution are disconnected from the internet and/or network.

10.2 Documentation requirements

Products must be provided with an installation, configuration and user manual.
The manuals must (if applicable) clearly highlight or state at least the following matters:

- Hoe How the product must be installed, connected (electrical connection diagram), configured and operated to meet the requirements / conditions set by SKG.
  It must also be indicated; how firmware updates are made available and how the user can perform them themselves.
  If there are operating methods that mean the product no longer meets the SKG requirements, this must be clearly indicated.

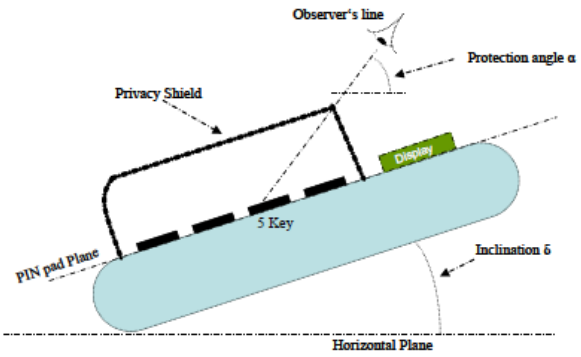
- Conditions for products with only the functional components 'Link D' and 'Actuator':
  - The SKG requirements are only met if the control of the products meets the requirements as stated in the applicable AE3104 and that the entire system complies with the basic system model should be considered.

- Conditions passive-power products (lock unlocked by power failure):
  - The SKG requirements are only met if a power failure is signalled to the user or an Alarm Center (e.g. PAC) and this power failure is covered by a suitable emergency power supply for at least 24 hours. The emergency power supply may be over-ruled by a fire or evacuation alarm.

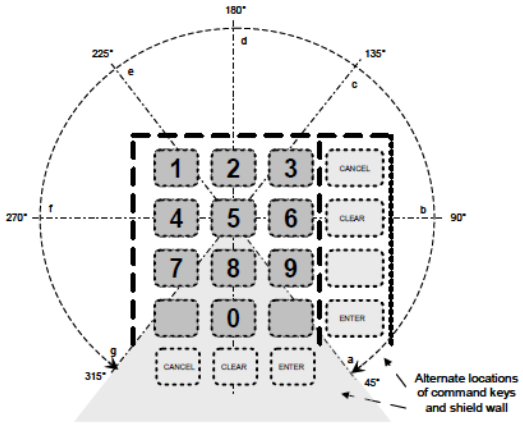
- Conditions for applying biometric readers:
  - The reader must meet 'Grade C' of the 'Credential related security' requirements as stated in EN 16867:2021: _ FAR-1 / max. number of auth. templates: 10.000
    _ Additional security features: alive detection

- Conditions for application of electronic keypads:
  - Clear warning that when using a keypad the certification is downgraded to SKG 2-star level.
  - Code length at least 4 digits and/or 4 characters.
  - If the product is applied in a public space; recording advice “regularly change the code”.
  - The keypad must be shielded in accordance with the requirements stated under 'Protected visibility' as stated in EN 16867:2021 (next page):

The height of the shielding is determined by a radius from the reference point (the 5 key and/or the center of the code panel) at an angle ≥ 30 degrees from the protection zone.



Shielding height



Protection zone

11 Evaluation and verification

The requirements as formulated in this document are tested on the basis of a self-declaration by the manufacturer of the product submitted for evaluation.

SKG-IKOB assesses the self-declaration for correctness and completeness. Furthermore, if products also contain a mechanical component covered by a standard(s) regularly used by SKG-IKOB, they must comply with the standard(s) in question. If test methods are linked to this, the product offered will also be subjected to these tests.

The product or combination of products submitted for assessment must comply with the self-declaration issued at the time of submission and during the lifetime of the product or combination of products. The party submitting a product for assessment to SKG-IKOB is fully responsible for the content of the self-declaration supplied and for the applicability of that self-declaration to the products as installed in the field.

11.1 Change of product

If changes are made after SKG-IKOB has granted a certificate for a product (system) and those changes affect the classified characteristics as described in this AE, an updated self-declaration must be submitted to SKG-IKOB. SKG-IKOB has the discretion to assess whether certification can be continued.

12 Model self-declaration

In addition to the standard test(s) for determining the burglar-proof properties and the quality requirements of the ‘Products’, the additional requirements are tested using a self-declaration. This declaration must be based on the ‘Model declaration’, see annex:

03 Product requirements for seam protectors on doors (lock side)

CvD decision: 07-12-10 / 06-09-12

Introduction
From NEN 5089 a manual test applies according to NEN 5096.
Seam protectors are not independently burglar-resistant and can only qualify for 1-star, if they are used with a lock.

Decision
The Board has decided that such products can be certified, provided that they meet specified criteria and are tested according to the protocol below;

1. Seam protector (frame and/or leaf section) must completely cover the closing seam.
2. Seam protector (parts that remain visible after assembly) must satisfy grade 3 of NEN-EN 1670:1998, the determination methods and acceptance conditions apply as described in section 5
3. Seam protector must be able to with stand a manual attack for 3 minutes (RC2) of contact time. Inward and outward-opening doors must be tested in the same way using the following determination method;

   Seam protector is fitted in accordance with the assembly instructions to a reference door, which is provided with a main lock, handle position 1050 mm and a side lock, position under the main lock*****.

   * *for the test, it is not necessary to actually install the locks, but the door must be closed and the positions of the (virtual) bolts marked.*

   The seam protector serves in the event of an attack, aimed at breaking loose from the bottom protector the closing seam so that the bolt of the main lock remains shielded.

4. Mounting conditions: application on doors with a main- and additional lock, of which at at least 1 of both SKG 1-star.

04 Marking conditions for emergency and panic devices

CvD decision: 09-04-09

Lock with an escape function may also be granted stars if they are demonstrably burglar resistant.
Because they cannot satisfy the requirement of lockability, testing does not include manipulation from the outside (drilling a hole).
In view of the vulnerability to manipulation, particular attention must be paid to this aspect when using such products.

These burglar-resistant (non-lockable) products must also be indelibly marked, directly under or beside the SKG mark, with:

- The pictogram for escape routes (stylistic) or
- The designation EN 179 or EN 1125.

Example of pictogram for escape routes:

05 Alternative provisions for durability & corrosion resistance of locks

CvD decision: 07-12-10

Introduction
For locks in NEN 5089 a reference is made for the aspect corrosion resistance and durability to European product standards;

A: Corrosion Resistance: grade C (digit 6)
This means a 96-hour salt spray test in accordance with EN 1670, after which the closure must still work. Section 5.4 of EN 1670 also specifies limits for the amount of rust developed on the visible parts. However, this section is omitted from EN 12209, the front plate of a closure may rust without a specified limit. Existing certified locks do satisfy (aesthetic) requirements of corrosion resistance because they were assessed in the past.

B: Durability: grade C (digit 2)
For locks this means an extensive test, for which the lock is fitted in a door and must withstand 200.000 cycles as a complete unit. This test is expensive because a test rig needs to be built, and time-consuming, about 2 weeks per lock.
Using the test equipment according to 2nd Draft. NEN 5089:1994 (operating speeds in accordance with EN standards), the locks are tested equivalent to the EN standards.

Decision
Item A. For locks and latches, the additional requirement applies that the parts that remain visible after assembly (e.g. the front plate) must at least satisfy the acceptance criteria of EN 1670 after the corrosion test.

Item B. Carry out the tests according to the methods of 2nd Draft NEN 5089:1994 with the following speeds:

I. Test latch, 16 operations/min. on a 6-fold test unit (carrousel).
II. Test deadbolt, 15 operations/min. on a 5-fold test unit.
III. Test latch mechanism, 30 operations/min. on a 6-fold test unit.


I. Latch


II. Deadbolt


III. Latch mechanism

06 Further explanation & criteria for manual testing

CvD decision: 09-04-09 / 16-03-11 / 22-10-14 / 30-03-16

Introduction
NEN 5089 states that the classification of building hardware takes place (among other things) on the basis of a manual test in accordance with NEN 5096 on façade elements selected in such a way that they correspond with the most common constructions used in both existing buildings and new building work.
These representative elements are defined in more detail but still fairly generally. For the purpose of certification by SKG-IKOB, specific facade element types are defined exactly, see the appendices to this document.
As a result of this, products classified in this way;

- Can be used in the context of the security guidelines for existing buildings.
- Can be used in facade elements described in a (KOMO or other) declaration of quality relating to the aspect burglar resistance.
- Can be used in facade elements described in the most recent version of the SKH publication 98-08.

SKG-IKOB-certified building hardware, used in accordance with the corresponding assembly instructions in wooden facade elements as described in the SKH publication 98-08 or in plastic or metal facade elements supplied under a (KOMO or other) declaration of quality, provides elements that satisfy RC 2 (or higher) of NEN 5096 (EN 1627). This means that the requirements for burglar resistance in the Dutch Buildings Decree are satisfied.

Further rules and conditions:
1. Tests for SKG-IKOB product certification are carried out in accordance with NEN 5096:2012***)***
2. The closing devices must be fitted on the side of the transom or mullion.
3. A hinge-set for use on windows and doors that are rotating inside and outside must be tested in its most critical application; (double)window opening outwards.
4. Flush-mounted products that can be used for opening in either direction are tested in the most critical direction. The test result applies to the other direction as well.
5. Surface mounted products that can be used for opening either inwards or outwards (different locking plates) must be tested in both directions.
6. Composite products (composite hardware / double door closures) which are suitable for both directions of opening must be tested in both directions.
7. Testing with 2 separate window closures; if the lower closing point remains intact for 3 minutes, the product may be used singly on a window with a max. height of 50 cm (PKVW BB)
8. Conformity or equivalence of building hardware products will be ascertained by SKG-IKOB.
9. Laboratory tests on building hardware products will be carried out by SKG-IKOB.
10. Manual building hardware tests will be carried out by SKG-IKOB in collaboration with SHR.
11. In principle, the test must be carried out on 2 elements (preliminary test and main test).
    It is acceptable to carry out just 1 test, but this must then be convincing (main test considered unnecessary).

) Explanation:

For the purpose of certification by SKG-IKOB, the criteria and working method for a manual test as described in NEN 5096 and the use of the tools available is defined, however the penetration opening and use of tools can lead to discussion and are defined and adhered to as follows;

_ *The penetration opening: 150x250x250 mm (NEN 5096) remains (instead of: 250x400 mm / EN 1627).*
_ *The available tools will not be used to deliberately assault the material of the construction with the object of manipulating the hardware.*
_ *The hacksaw (tool set A2), supplemented with the bench hammer (200g) and a punch set may only be Used for attacking hinge pins.*

_ *Attack of gratings/barrier facilities using the hacksaw will be as yet excluded, therefore they do not automatically meet the level RC2 or higher for complete façade elements (new construction).*
_ *For the tools that are not specified in detail (tool-set A1), it is assumed that these are reasonably easy for anyone to obtain, cost very little and require no preparations.*
These are explained in more detail as follows;

Rope and steel wire:
- wire (up to max. 4mm), including electrical wire, cables, washing line etc.
- any kind of rope or string
- any kind of generally available rubber bands

Adhesive tape:
- any kind of adhesive tape

Set of small screwdrivers: (max. length 250mm)
- slit up to 6 mm
- pozidrive head up to no.PZ3
- Philips head up to no. PH3

Hexagonal keys: (incl. bit-holder and bits)
- torx up to T40
- hex up to 6 mm

Pliers: (max. length 180 mm)
- combination pliers 180 mm
- straight locking pliers 150 mm
- angled locking pliers 150 mm

Remark: *Where preparation of supplementary tools is an option, it's only permitted with the resources available from the toolset A1.*

07 Product requirements for code locks

CvD decision: 20-11-19

Introduction

NEN 5089 does not provide the possibility or requirements for lockability by means of code locking. However, there are burglary resistant products with such a locking mechanism, which can reasonably be used, provided that various conditions are met.

Decision

The Board of Experts has determined that products with a code lock are **only** eligible for certification according SKG 1- or 2-star and has drawn up the following requirements for this.

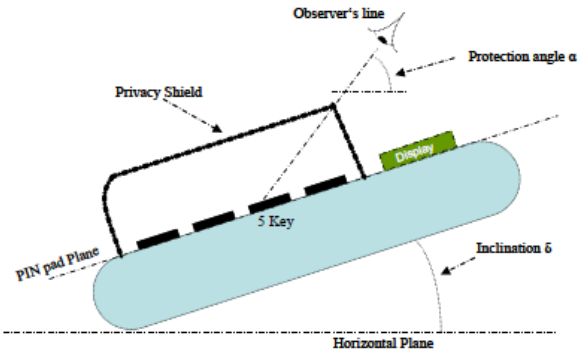
Requirements[a)]

- Number of close variations ≥ 10.000 *(see calculation examples below)*;
  - I. Lock type: with fixed code sequence: a code of at least 4 positions applies.
  - II. Lock type: with random code input: the code length range depends on the number of actual locking variations.
- Coding is not allowed due to visible wear on the knobs (well in or under allowed).
- Code should not remain visible after closing ***OR*** product may not close at pre-set code.
- Code Adjustable only from the secure side.
- If the product is used in a public space in the assembly- / instruction manual must be the advice; User group up to maximum 5 people and regularly change the code.
- The keypad must be durable[b)] shielded and must satisfy the guidelines of the; European Payments Council: EPC343-08 Version 1.4 approved, Par. 4.2.

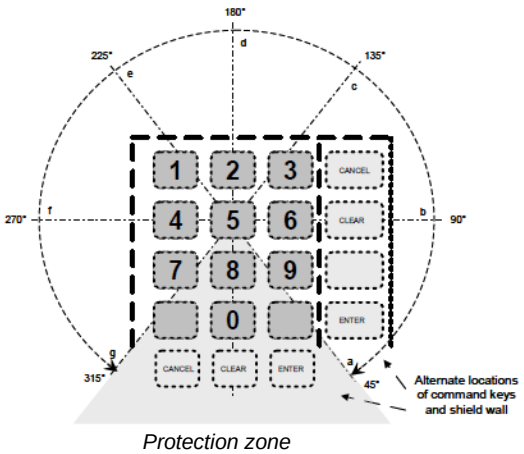
[a)] for electronic code locks the requirements of NO 02, par. 8 apply.
[b)] product and cannot be dismantled without visual changes (damage).

Par. 4.2 - mechanical requirements for the protective shield, horizontal and vertical installation;

- *The height of the privacy shield is determined by a radius from the reference point (the 5-key and/or the centre of the keypad) at an angle ≥ 40 degrees from the protection zone.*



Height privacy shield



Protection zone

Calculation examples

I. ***Lock type: with fixed code sequence***

Image : *code lock*

Example : *Total number of variations is achieved by the number of positions (^{Y}) and the number of different codes (blocking variants) (X).*
Formula : *Exponentiation: X^{Y} = number of variations.*
Calculation example: Number of positions 4 (^{Y}), per positions 10 variations (X)
10^{4} = 10.000 variations (≥ 10.000)

II. ***Lock type: with random code input***

Image : *code lock*

Example : *Total number of variations is reached by the sum of the variations of the total number of positions($_{n}$) per code length($_{k}$)*
Formula : *Faculty with set back: $\frac{n!}{k!\,(n-k)!}$ = number of variations per code length($_{k}$)*
Variations total = Σ number of variations per (allowed) code lengths($_{k}$)
*Calculation example: Total number of positions 14 ($_{n}$): **code length - min. 5 en max. 9 positions ≥ 10.000***

1 $\frac{14!}{1!\,(14-1)!}$ = 14

2 $\frac{14!}{2!\,(14-2)!}$ = 91

3 $\frac{14!}{3!\,(14-3)!}$ = 364

4 $\frac{14!}{4!\,(14-4)!}$ = 1001

5 $\frac{14!}{5!\,(14-5)!}$ **= 2002**

6 $\frac{14!}{6!\,(14-6)!}$ **= 3003**

7 $\frac{14!}{7!\,(14-7)!}$ **= 3432** ***code length 5 - 9 = 13442 variations (≥ 10.000)***

8 $\frac{14!}{8!\,(14-8)!}$ **= 3003**

9 $\frac{14!}{9!\,(14-9)!}$ **= 2002**

10 $\frac{14!}{10!\,(14-10)!}$ = 1001

11 $\frac{14!}{11!\,(14-11)!}$ = 364

12 $\frac{14!}{12!\,(14-12)!}$ = 91

13 $\frac{14!}{13!\,(14-13)!}$ = 11

14 $\frac{14!}{14!\,(14-14)!}$ = 1 +

Total = 16380 variations

08 Product requirements for mechatronic padlocks

CvD decision: 17-04-23

Introduction

Requirements for padlocks are included in NEN 5089, which among other, refers to the European product standard for mechanical padlocks EN12320:2021.
There is also a European product standard EN 16864:2017 for mechatronic padlocks, which includes identical mechanical aspects and additional electronic aspects.

Decision

In addition to the requirements in NEN 5089 that are not included in the European product standard, the requirements for mechanical and electronic aspects also apply, insofar as these are comparable to resp. mechanical padlocks and electromechanical cylinders.
This results in the following declaration according to EN 16864;

Specific requirements to mechatronic padlocks

	1	2	3	4	5	6	7	8
	Category of use	Durability	Corrosion resistance	Environmental resistance	Mechanical key related security	Electronic key related security	System management	Attack resistance
SKG 1-ster	-	-	3	3	3	B	-	3
SKG 2-ster					4	C		4 (> 55 kN)
SKG 3-ster					5	D		5 (> 80 kN)

MODEL SELF-DECLARATION

Self-declaration
[Company name], as listed under “Details of the ‘Applicant’”, hereinafter referred to as ‘Applicant’, validly represented in this matter by **[name of person]**, whose contact details are listed under “Details of the ‘Respondent’ and hereinafter referred to as ‘Responsible Person’, has submitted a request to SKG-IKOB to carry out certification of the product (system) as listed under “5.2 The ‘Products’ to which this self-declaration applies”, hereinafter referred to as ‘Products’, even if it concerns only one product.

The ‘Applicant’ has appointed **[name of contact person]**, whose contact details are listed under “Contact person of the ‘Applicant’” and hereinafter referred to as ‘Contact Person’, to liaise with SKG-IKOB in respect of the certification request submitted to SKG-IKOB and to handle the process on behalf of the ‘Applicant’.

As part of the certification application, the ‘Applicant’ is expected to submit a self-declaration to SKG-IKOB, in which it is stated by the ‘Applicant’ that the ‘Products’ comply with the requirements as stated in AE 3104_17-04-2024, “Additional requirements relating to Electromechanical and Electronic Building Hardware”.

In addition to the self-declaration, the installation and operating instructions of the ‘Products’ are expected to be provided to SKG-IKOB. The ‘Applicant’ has attached these documents, provided with version indications, as annexes to this self-declaration. An overview of the added enclosures is given under “Enclosures attached by ‘Applicant’:”

Details of the ‘Applicant’

Company name	:
Address	:
Postcode	:
Place of business	:
Country	:
Phone number	:
CoC number	:

Details of the ‘Respondent’

Name	:
Position	:
Phone number	:
E-mail address	:

Contact person of the ‘Applicant’

Name	:
Position	:
Phone number	:
E-mail address	:

5.2 The 'Products' to which this self-declaration applies*):

All 'Products' covered by this self-declaration and for which the request for certification has been submitted to SKG are listed below.

Product name :
Type number :
Firmware version :

***)** *If the product is a composition of products and/or services, the above must be indicated for each product and/or service offered. When SKG-IKOB request multiple copies of a certain product, each copy must be indicated separately.*

Enclosures attached by 'Applicant':

The following enclosures are included as part of the self-declaration:

State here the user and installation manual(s) of the 'Products' (document name with version number).

The 'Products' received by SKG-IKOB

☐ The 'Applicant' declares that the copies of the 'Products' submitted to SKG-IKOB correspond exactly to the 'Products' as offered on the market.

☐ The 'Applicant' declares that the copies of the 'Products' submitted to SKG-IKOB do not correspond exactly to the 'Products' as offered on the market.
The deviations and an explanation of why there are these deviations are given below:

If one or more products and/or services deviate from what is offered on the market, please explain here what the deviation is and why it exists.

A short description of the 'Products' (according to the basic system model)

Provide here a short (maximum 1 A4) description of the product, clearly showing the purpose of the product and its functionality. If the product is a combination of products and/or services, the connection must be clear from the description.

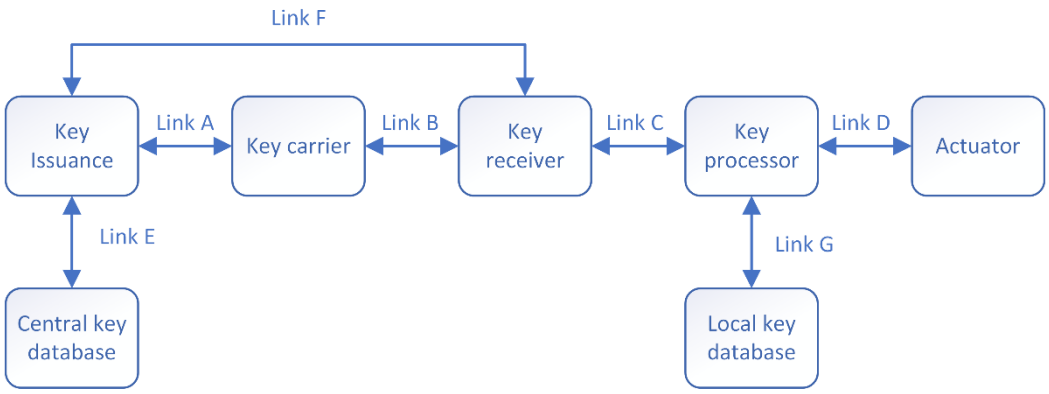


Figure 2: The basic system model

5.3 Requirements for signal transmission

'Link A':

☐ 'Link A' is not relevant to the 'Products' because:

Indicate here in a short description why this component is not relevant to the product.

☐ 'Link A' is relevant to the 'Products', meets all the additional requirements set for this link and conforms to the following type in 'Table 1' of AE 3104:

- ☐ Internal, contact. Product in secure zone.
- ☐ Internal, contact. Product in unsecured zone.
- ☐ External, contact, secure zone.
- ☐ External, contact, unsecured zone.
- ☐ Wireless.
- ☐ Public networks.

'Link B':

☐ 'Link B' is not relevant to the 'Products' because:

Indicate here in a short description why this component is not relevant to the product.

☐ 'Link B' is relevant to the 'Products', meets all the additional requirements set for this link and conforms to the following type in 'Table 1' of AE 3104:

- ☐ Internal, contact. Product in secure zone.
- ☐ Internal, contact. Product in unsecured zone.
- ☐ External, contact, secure zone.
- ☐ External, contact, unsecured zone.
- ☐ Wireless.
- ☐ Public networks.

'Link C':

☐ 'Link C' is not relevant to the 'Products' because:

Indicate here in a short description why this component is not relevant to the product.

☐ 'Link C' is relevant to the 'Products', meets all the additional requirements set for this link and conforms to the following type in 'Table 1' of AE 3104:

- ☐ Internal, contact. Product in secure zone.
- ☐ Internal, contact. Product in unsecured zone.
- ☐ External, contact, secure zone.
- ☐ External, contact, unsecured zone.
- ☐ Wireless.
- ☐ Public networks.

'Link D':

☐ 'Link D' is not relevant to the 'Products' because:

Indicate here in a short description why this component is not relevant to the product.

☐ 'Link D' is relevant to the 'Products', meets all the additional requirements set for this link and conforms to the following type in 'Table 1' of AE 3104:

- ☐ Internal, contact. Product in secure zone.
- ☐ Internal, contact. Product in unsecured zone.
- ☐ External, contact, secure zone.
- ☐ External, contact, unsecured zone.
- ☐ Wireless.
- ☐ Public networks.

'Link E':

- [ ] 'Link E' is not relevant to the 'Products' because:

Indicate here in a short description why this component is not relevant to the product.

- [ ] 'Link E' is relevant to the 'Products', meets all the additional requirements set for this link and conforms to the following type in 'Table 1' of AE 3104:
  - [ ] Internal, contact. Product in secure zone.
  - [ ] Internal, contact. Product in unsecured zone.
  - [ ] External, contact, secure zone.
  - [ ] External, contact, unsecured zone.
  - [ ] Wireless.
  - [ ] Public networks.

'Link F':

- [ ] 'Link F' is not relevant to the 'Products' because:

Indicate here in a short description why this component is not relevant to the product.

- [ ] 'Link F' is relevant to the 'Products', meets all the additional requirements set for this link and conforms to the following type in 'Table 1' of AE 3104:
  - [ ] Internal, contact. Product in secure zone.
  - [ ] Internal, contact. Product in unsecured zone.
  - [ ] External, contact, secure zone.
  - [ ] External, contact, unsecured zone.
  - [ ] Wireless.
  - [ ] Public networks.

'Link G':

- [ ] 'Link G' is not relevant to the 'Products' because:

Indicate in a short description why this component is not relevant to the product.

- [ ] 'Link G' is relevant to the 'Products', meets all the additional requirements set for this link and conforms to the following type in 'Table 1' of AE 3104:
  - [ ] Internal, contact. Product in secure zone.
  - [ ] Internal, contact. Product in unsecured zone.
  - [ ] External, contact, secure zone.
  - [ ] External, contact, unsecured zone.
  - [ ] Wireless.
  - [ ] Public networks.

5.4 Requirements for access to and storage of key data

'Key issuance':

☐ The 'Key issuance' component is not relevant for the 'Products' because:

Indicate here in a short description why this component is not relevant to the product.

☐ The component 'Key issuance' is relevant to the 'Products' and meets the requirements from 'Table 2' of AE 3104. This component is implemented as follows:

Give here a short description indicating how this component has been implemented for the product. Indicate clearly how any management application(s) can be accessed and used by SKG-IKOB for the purpose of an inspection.

'Central key database':

☐ The 'Central key database' component is not relevant for the 'Products' because:

Indicate here in a short description why this component is not relevant to the product.

☐ The component 'Central key database' is relevant to the 'Products' and meets the requirements from 'Table 2' of AE 3104. This component is implemented as follows:

Give here a short description indicating how this component has been implemented in the product. Indicate clearly where the 'Central key database' is stored. If this is in an external data centre, also provide the information on that data centre.

'Key carrier':

☐ The 'Key carrier' component is not relevant for the 'Products' because:

Indicate here in a short description why this component is not relevant to the product.

☐ The component 'Key carrier' is relevant to the 'Products' and meets the requirements from 'Table 2' of AE 3104. This component is implemented as follows:

Give here a short description indicating how the component 'Key carrier' has been implemented in the product. If there can be several 'Key carriers', clearly state which variants they are and how each variant has been implemented.

'Key Receiver':

☐ The 'Key receiver' component is not relevant for the 'Products' because:

Indicate here in a short description why this component is not relevant to the product.

☐ The component 'Key receiver' is relevant to the 'Products' and meets the requirements from 'Table 2' of AE 3104. This component is implemented as follows:

Give here a short description indicating how the component 'Key receiver' has been implemented in the product. If there can be several 'Key receivers', clearly state which variants they are and how each variant has been implemented.

'Key processor':

☐ The 'Key processor' component is not relevant for the 'Products' because:

Indicate here in a short description why this component is not relevant to the product.

☐ The component 'Key processor' is relevant to the 'Products' and meets the requirements from 'Table 2' of AE 3104. This component is implemented as follows:

Give here a short description indicating how the component 'Key processor' has been implemented in the product.

'Local key database':

- ☐ The 'Local key database' component is not relevant for the 'Products' because:

Indicate her in a short description why this component is not relevant to the product.

- ☐ The component 'Local key database' is relevant to the 'Products' and meets the requirements from 'Table 2' of AE 3104. This component is implemented as follows:

Give here a short description indicating how the component 'Local key database' has been implemented in the product.

'Actuator':

- ☐ The 'Actuator' component is not relevant for the 'Products' because:

Indicate here in a short description why this component is not relevant to the product.

- ☐ The component 'Actuator' is relevant to the 'Products' and meets the requirements from 'Table 2' of AE 3104. This component is implemented as follows:

Give here a short description indicating how the component 'Actuator' has been implemented in the product.

5.5 Storage of passwords and keys

- ☐ Passwords are not stored for and/or by the 'Products' and/or the associated (management) systems and cannot be traced in any way.
- ☐ Keys transferable by a person, such as, but not limited to PIN codes and biometric data, are not stored for and/or by the 'Products' and/or the associated (management) systems and are not traceable in any way.
- ☐ Passwords and keys transferable by individuals cannot be accessed or viewed by any user or administrator at any level.

5.6 Operation

The 'Products' can be operated as referred to in AE 3104 in the following way(s):

- ☐ Direct control
- ☐ Local control
- ☐ Remote control

The implementation and/or execution of the possible operating modes:

- ☐ Meets all the requirements.
- ☐ Does not meet or does not fully meet all the requirements. The space below is used to explain and/or explain the deviations.

Please indicate here in a brief description how and why the completion deviates from the additional requirements set.

6 Software and firmware requirements

- ☐ All software belonging to the 'Products' that are part of the basic system model as referred to in AE 3104 meets the requirements. This has been done as follows:

Please give here a short description of how the additional requirements have been met.

- ☐ The firmware of the 'Products' and its updating meet all requirements as stated.

7 Requirements for digital keys

- [ ] The keys that can be used for the 'Products' and that fall into the category "Keys to be entered or transferred by a person", as referred to in AE 3104, comply with all requirements.
- [ ] There are no keys for the 'Products' that fall into the category of "Keys to be introduced or transferred by a person" as referred to in AE 3104.
- [ ] The keys that can be used for the 'Products' and that fall into the category of "Keys to be introduced or transferred by technology", as referred to in AE 3104, comply with all requirements.
- [ ] No keys exist for the 'Products' that fall into the category of "Keys to be introduced or transferred via technology" referred to in AE 3104.

8 Requirements for electronic keypads

- [ ] An electronic keypad is not part of and does not belong to the offered 'Products', nor can it be optionally added to the 'Products'.
- [ ] An electronic keypad is not part of and does not belong to the offered 'Products'. However, the option to optionally link an electronic keypad to the 'Products' does exist.
  The 'Products' and associated documentation meet the requirements.
- [ ] An electronic keypad belongs to or is part of the 'Products' offered. It is a standard method for entering keys or PIN codes, it and meets all the requirements stated.
- [ ] An electronic keypad belongs to or is part of the 'Products' offered. It is an optional method for entering keys or PIN codes and meets all the requirements.

9 Requirements for biometric readers

- [ ] A biometric reader is not part of and does not belong to the offered 'Products', nor can it be optionally added to the 'Products'.
- [ ] A biometric reader is not part of and does not belong to the offered 'Products'.
  However, the option to optionally link a biometric reader to the 'Products' does exist.
  The associated documentation meets the requirements.
- [ ] A biometric reader is part of or belongs to the 'Products' offered and meets all the requirements.

10 Other requirements

- [ ] The 'Product' and documentation complies with all 'Other Requirements' as stated.

Signature

The 'Applicant' declares that:

- this (the present) document is the self-declaration as referred to in AE 3104_17-04-2024;
- this self-declaration has been completed truthfully;
- The 'Applicant' will cooperate with any review of this declaration.

Duly signed on behalf of the applicant by:

Signature: ……

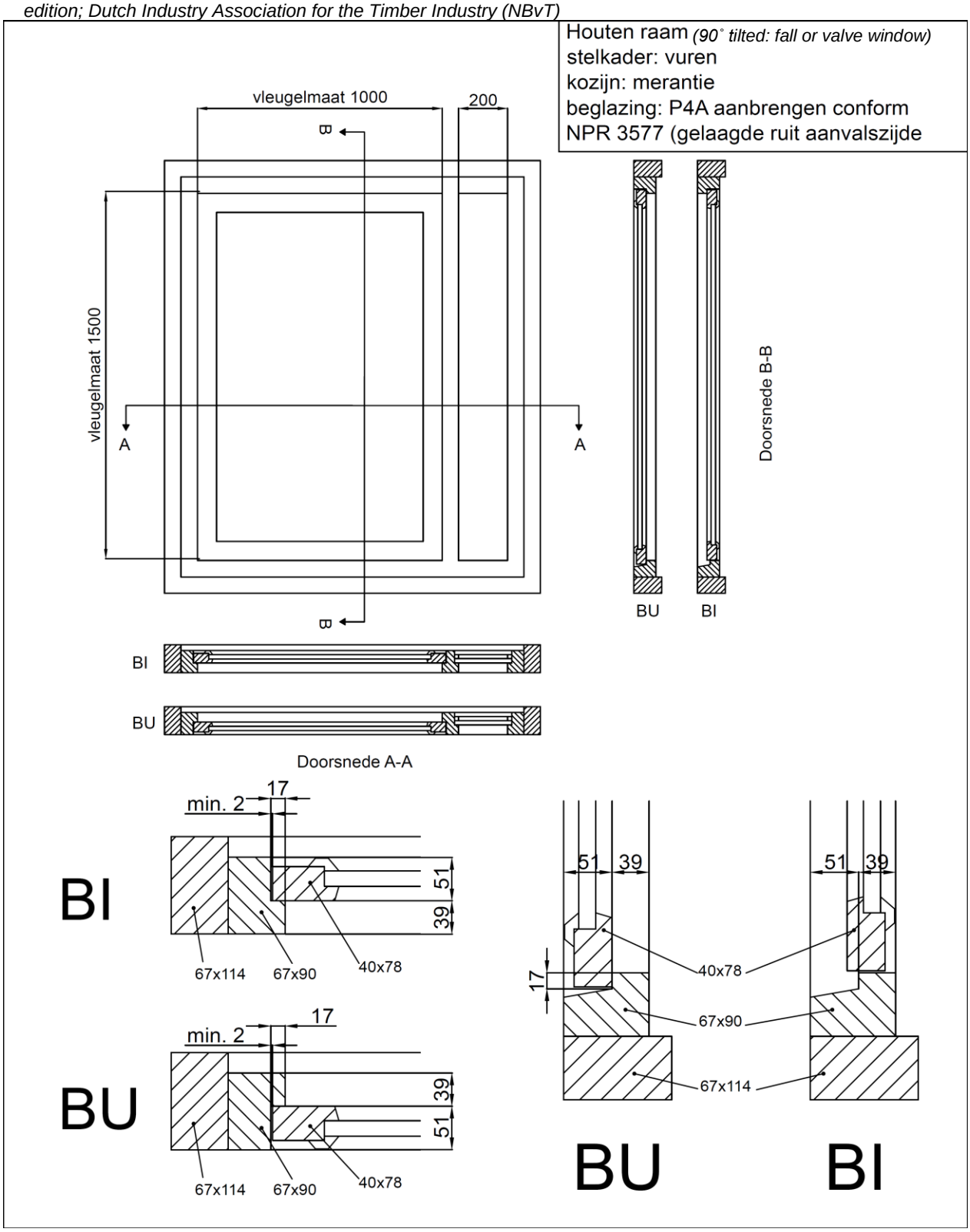
Name: ……

Position: ……

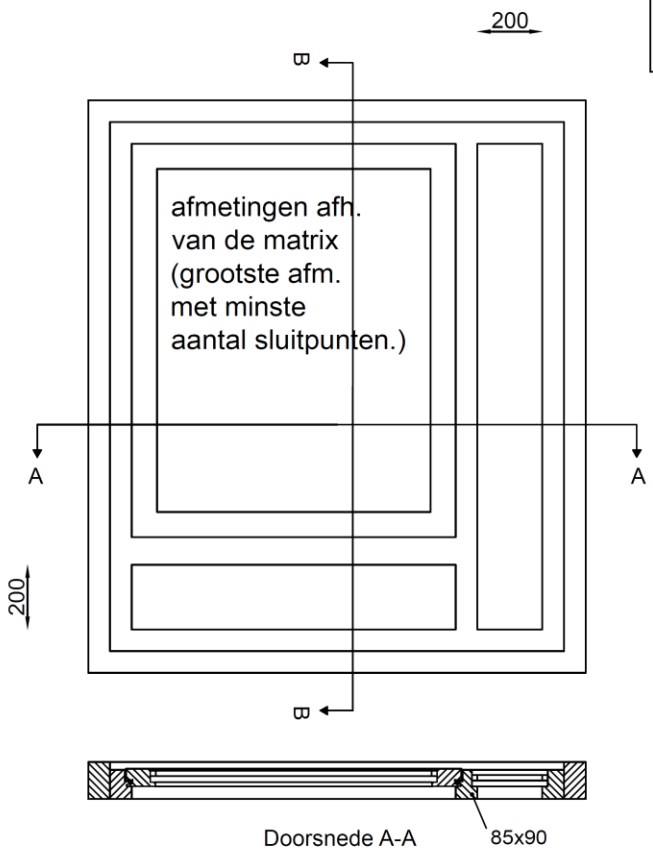
Date: ……

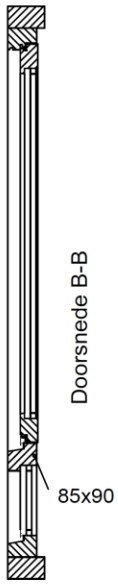
Wood*) 3 minutes (2-star)

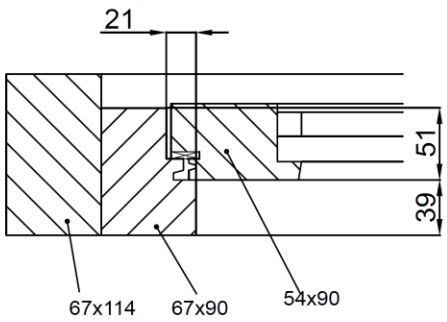
*) *Profile details as well as hanging- and closing seams must be executed in accordance with the KVT, edition; Dutch Industry Association for the Timber Industry (NBvT)*

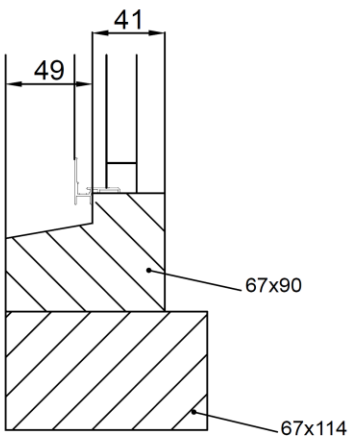


Houten draaivalraam 3 minuten
stelkader: vuren
kozijn: merantie
beglazing: P4A aanbrengen conform NPR 3577 (gelaagde ruit aanvalszijde)



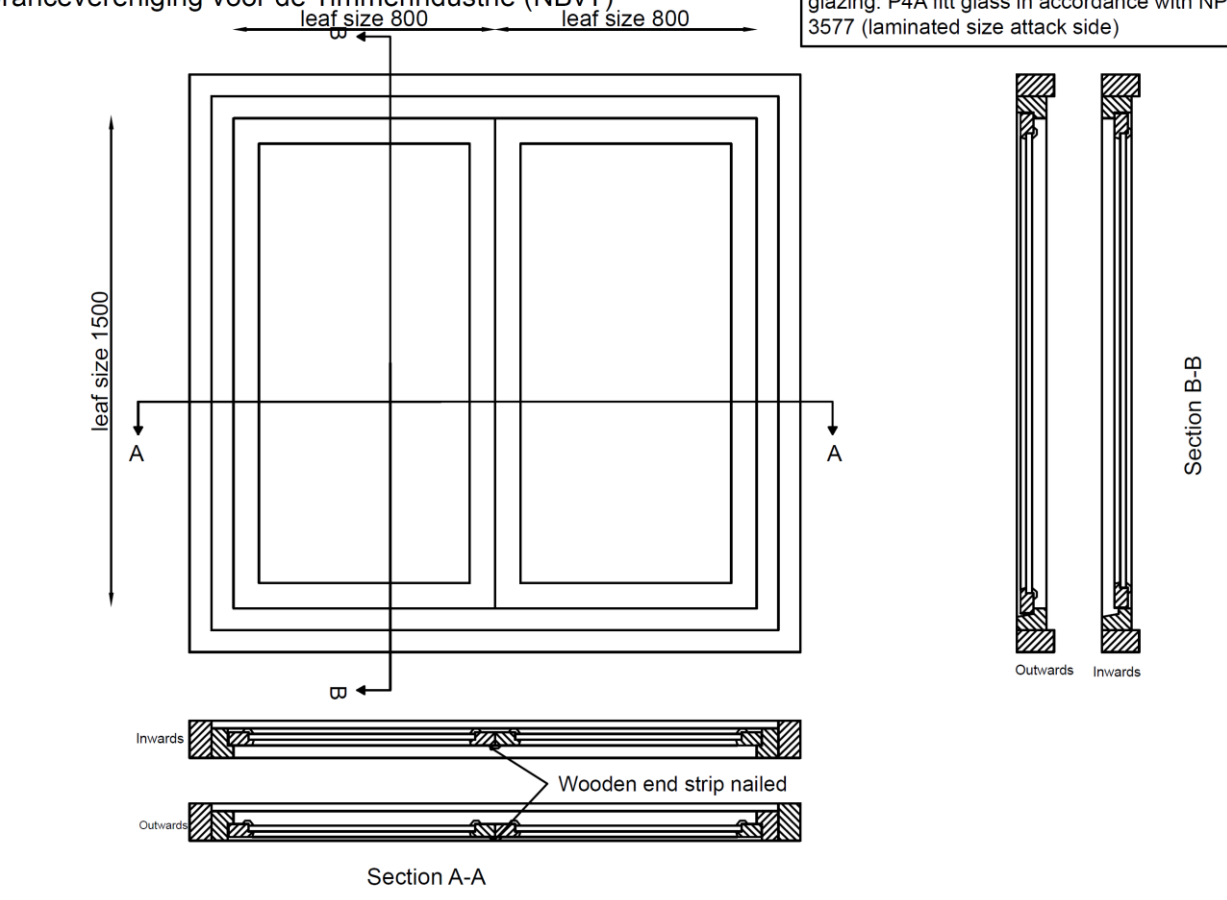


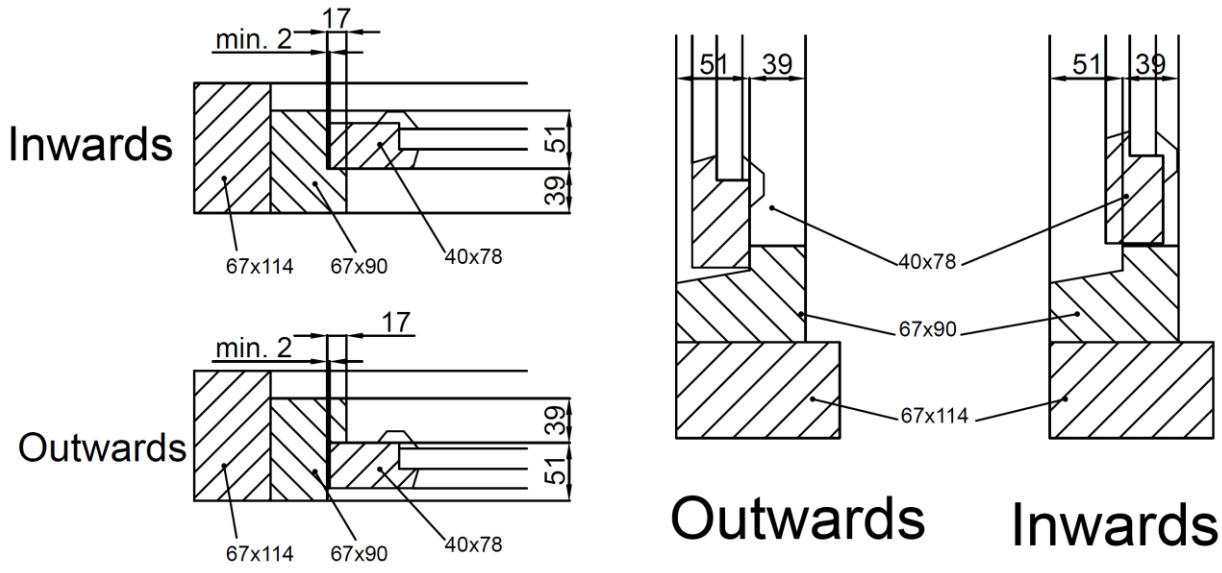




Frame details as well as hardware and seams should be carried out in accordance with the KVT, edition; Nederlandse Brancevereniging voor de Timmerindustrie (NBvT)

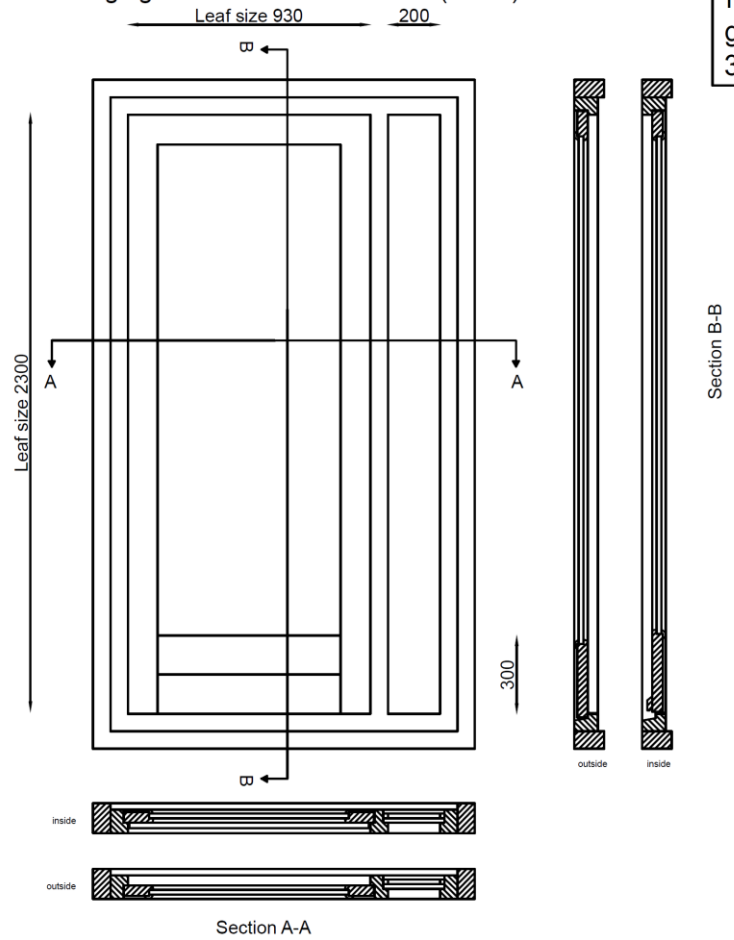
Wooden double window: 3 minuten
placement frame: pine wood
frame: merantie
glazing: P4A fitt glass in accordance with NPR 3577 (laminated size attack side)

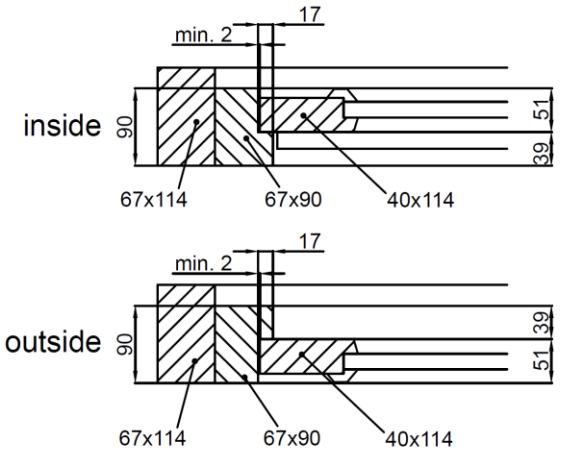


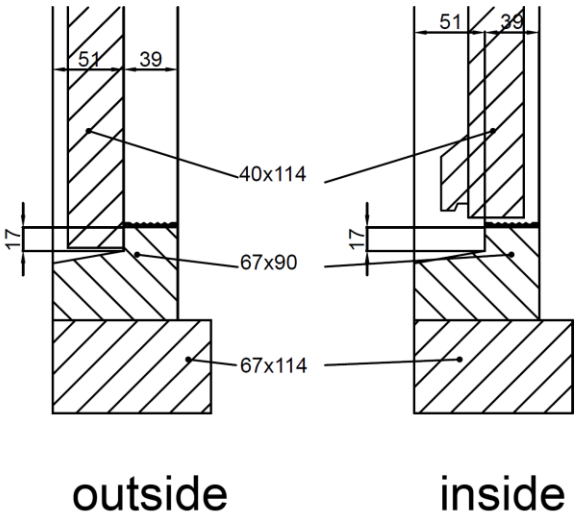


Frame details as well as hardware and seams should be carried out in accordance with the KVT, edition; Nederlandse Brancevereniging voor de Timmerindustrie (NBvT)

Wooden door: 3 minuten
placement framework:pine wood
frame: meranti
glazing: P4A in accordence with NPR 3577 (laminated glass is attack side)

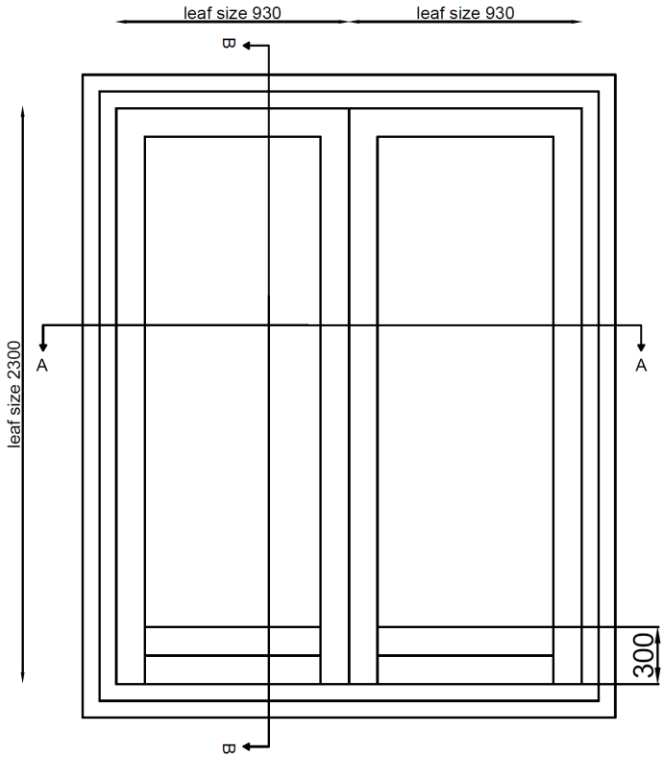




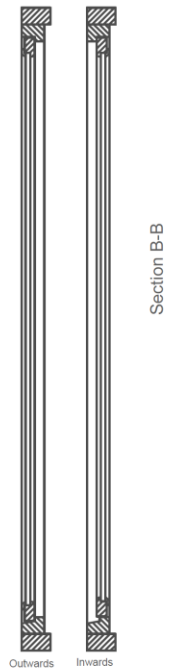


Frame details as well as hardware and seams should be carried out in accordance with the KVT, edition; Nederlandse Brancevereniging voor de Timmerindustrie (NBvT)

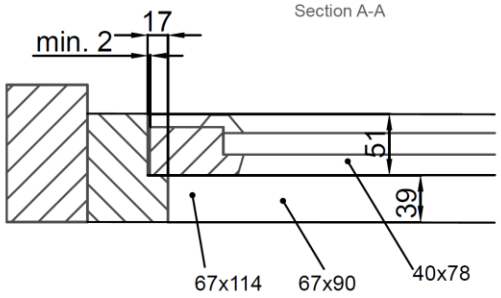
wooden double door: 3 minutes
placement framework: pine wood
frame: merantie
glazing: P4A fitt glass in accordance with NPR 3577
(laminated side is attack side)

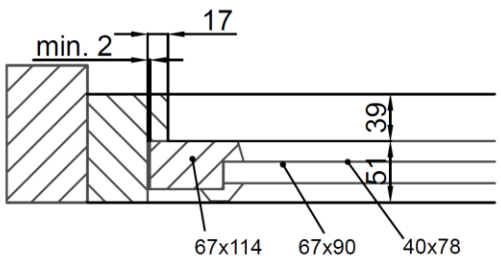


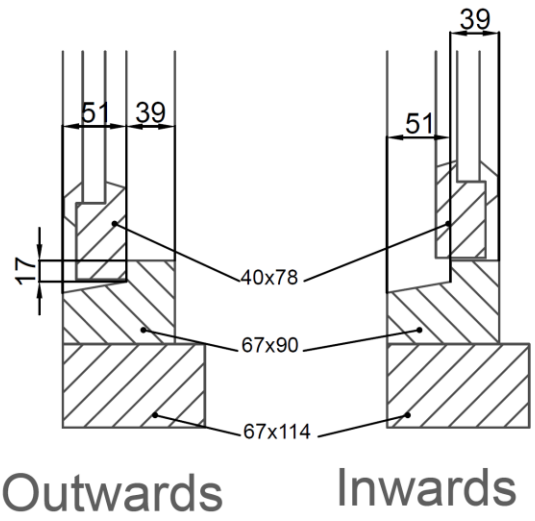
Section A-A



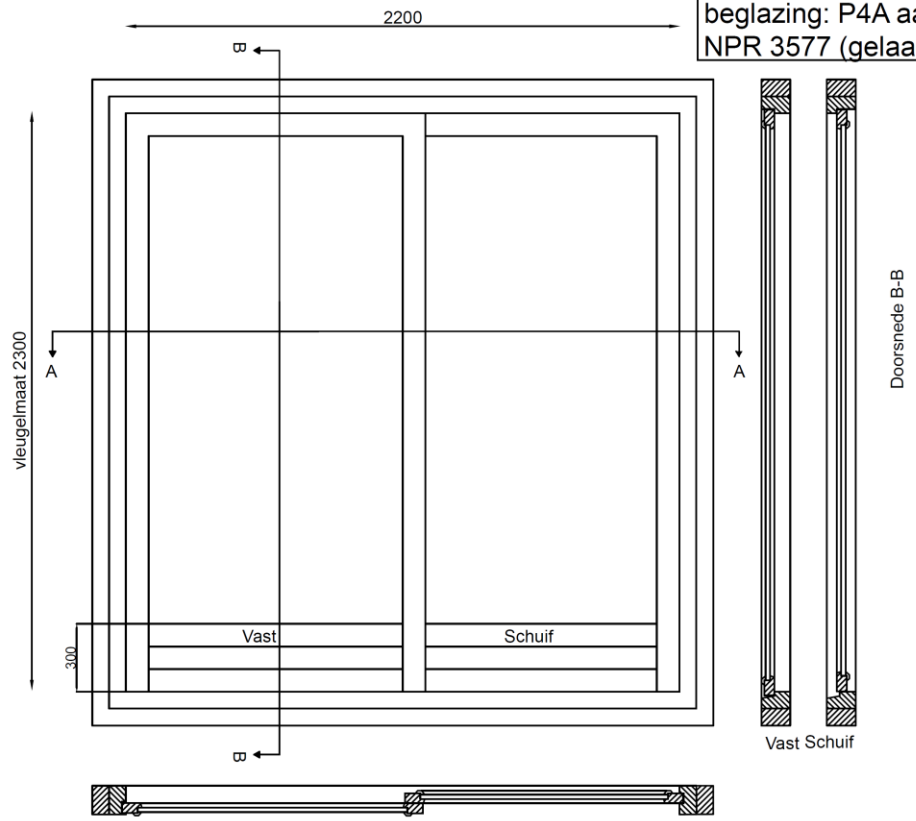
Section B-B



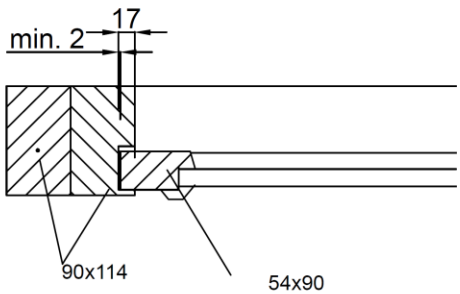


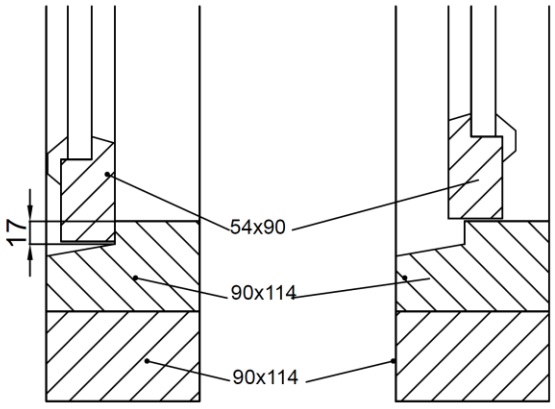


Houten schuifdeur (bi) 3 / 5 min
stelkader: vuren
kozijn: merantie (3min) / sapeli (5 min)
beglazing: P4A aanbrengen conform NPR 3577 (gelaagde ruit aanvalszijde)



Doorsnede A-A

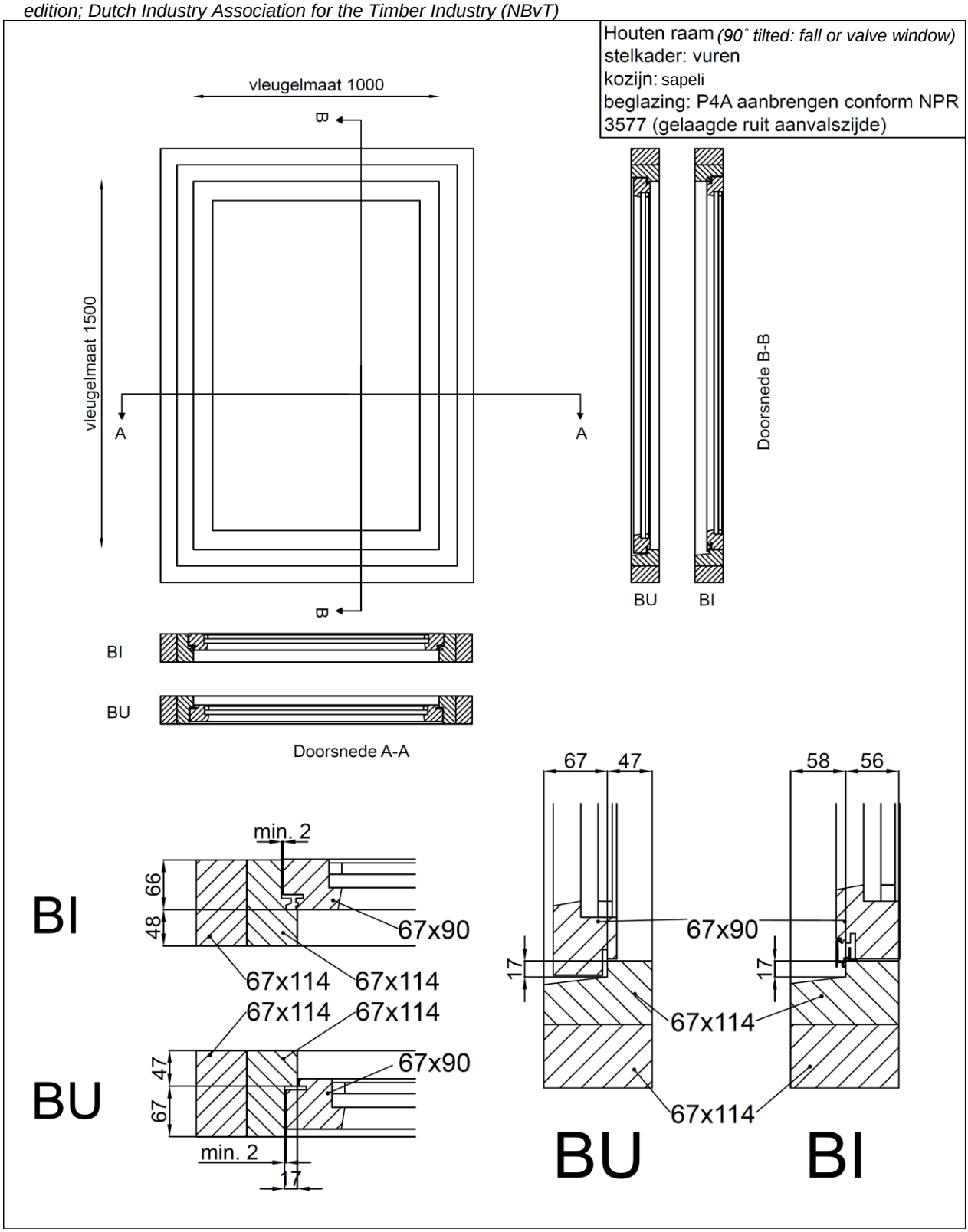




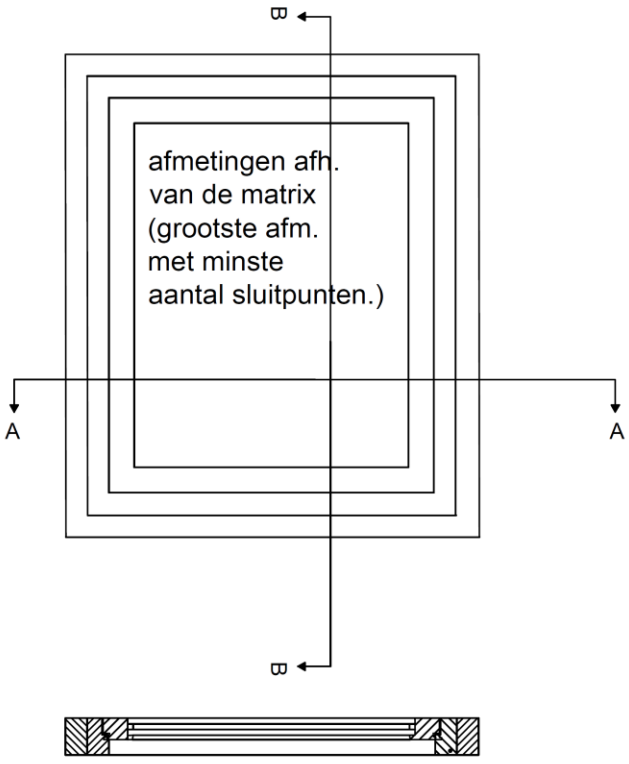
Vast Schuif

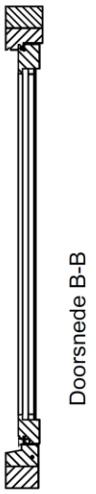
Wood*) 5 minutes (3-star)

*) *Profile details as well as hanging- and closing seams must be executed in accordance with the KVT, edition; Dutch Industry Association for the Timber Industry (NBvT)*

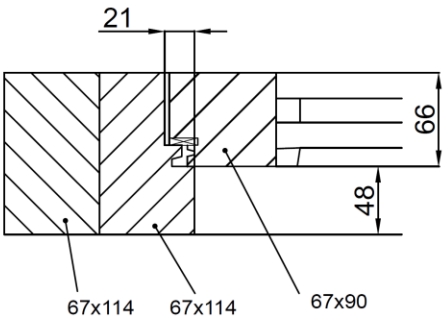


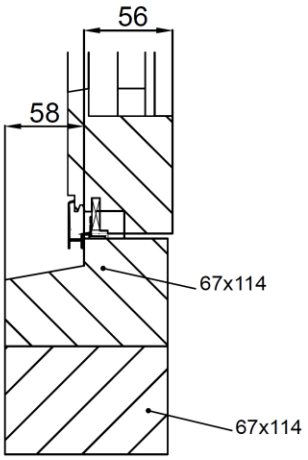
Houten draaivalraam 5 minuten
stelkader: vuren
kozijn: sapeli
beglazing: P4A aanbrengen conform NPR 3577 (gelaagde ruit aanvalszijde)





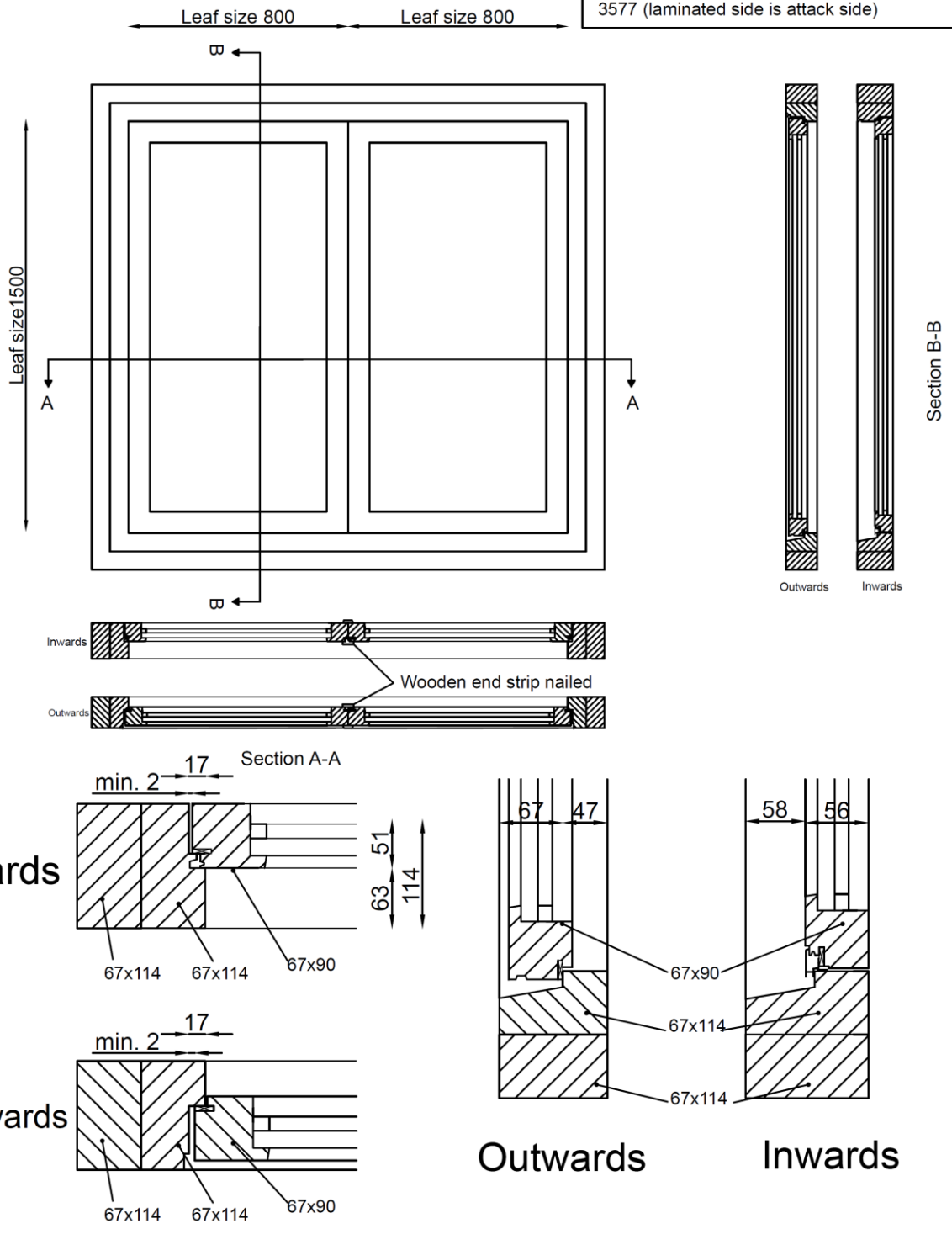
Doorsnede A-A





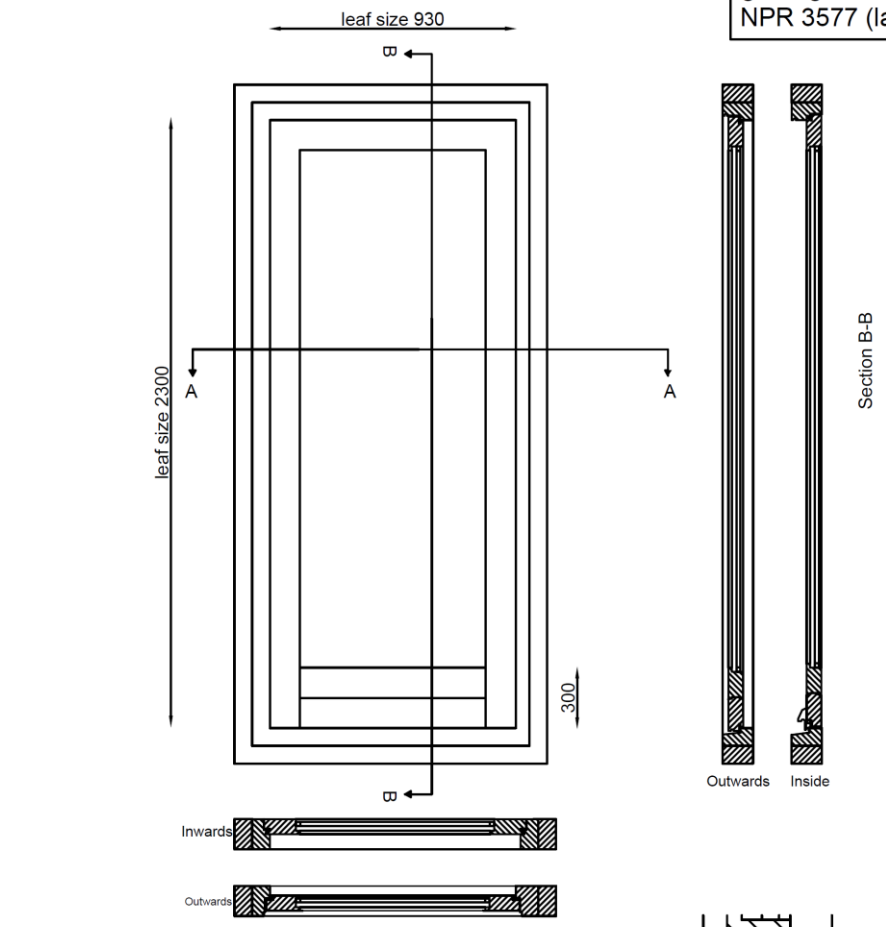
Frame details as well as hardware and seams should be carried out in accordance with the KVT, edition; Nederlandse Brancevereniging voor de Timmerindustrie (NBvT)

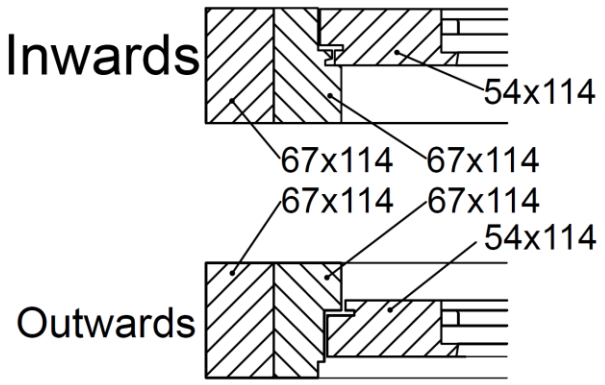
Wooden double window: 5 minuten
placement framework: pine wood
frame: sapeli
glazing: P4A fitt glass in accordance with NPR 3577 (laminated side is attack side)

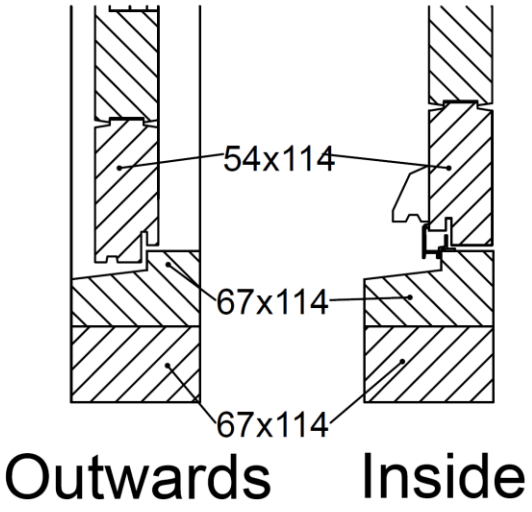


Frame details as well as hardware and seams should be carried out in accordance with the KVT, edition; Nederlandse Brancevereniging voor de Timmerindustrie (NBvT)

Wooden door: 5 minuten
placement frame: pine wood
frame: sapeli
glazing: P4A fitt glass in accordance with NPR 3577 (laminated side is attack side)

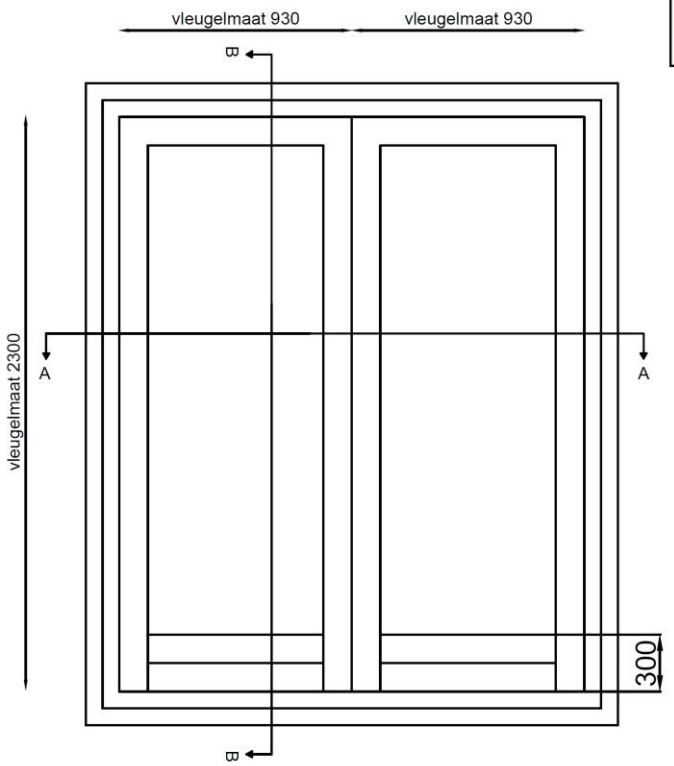




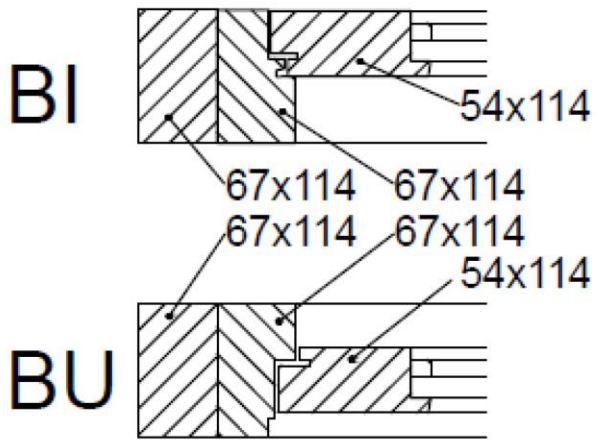


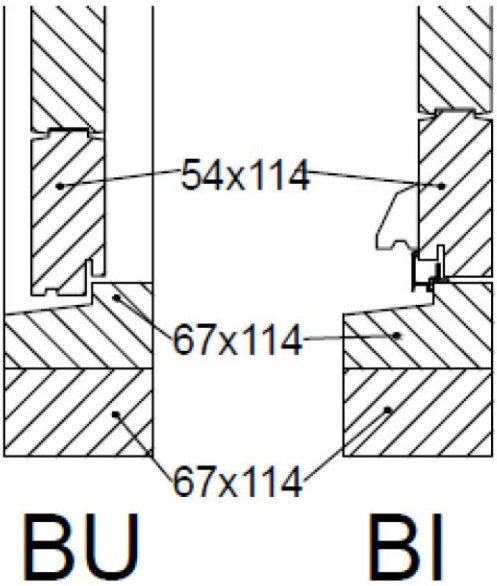
Profieldetails evenal hang- en sluitnaden dienen te worden uitgevoerd conform de KVT, uitgave; Nederlandse Brancevereniging voor de Timmerindustrie (NBvT)

Houten stolpdeur 5 minuten
stelkader: vuren
kozijn: sapeli
beglazing: P4A aanbrengen conform NPR 3577
(gelaagde ruit aanvalszijde)

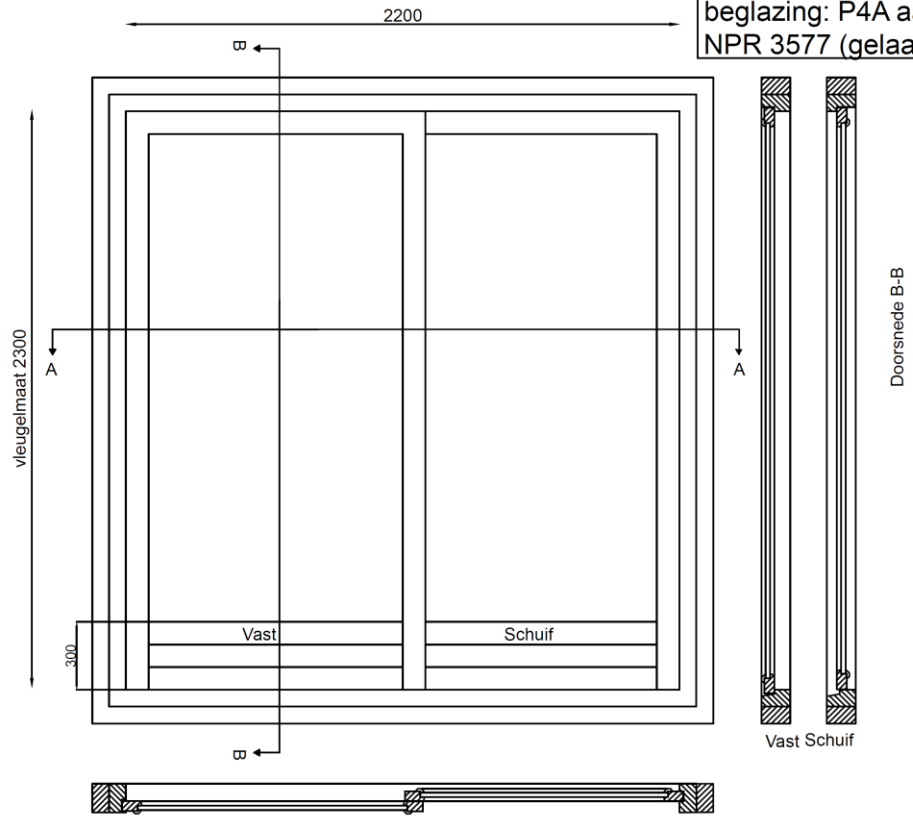


Doorsnede A-A

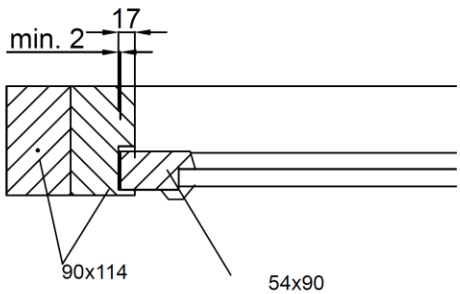


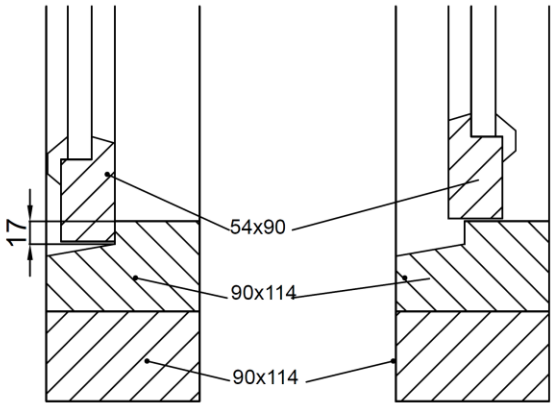


Houten schuifdeur (bi) 3 / 5 min
stelkader: vuren
kozijn: merantie (3min) / sapeli (5 min)
beglazing: P4A aanbrengen conform NPR 3577 (gelaagde ruit aanvalszijde)



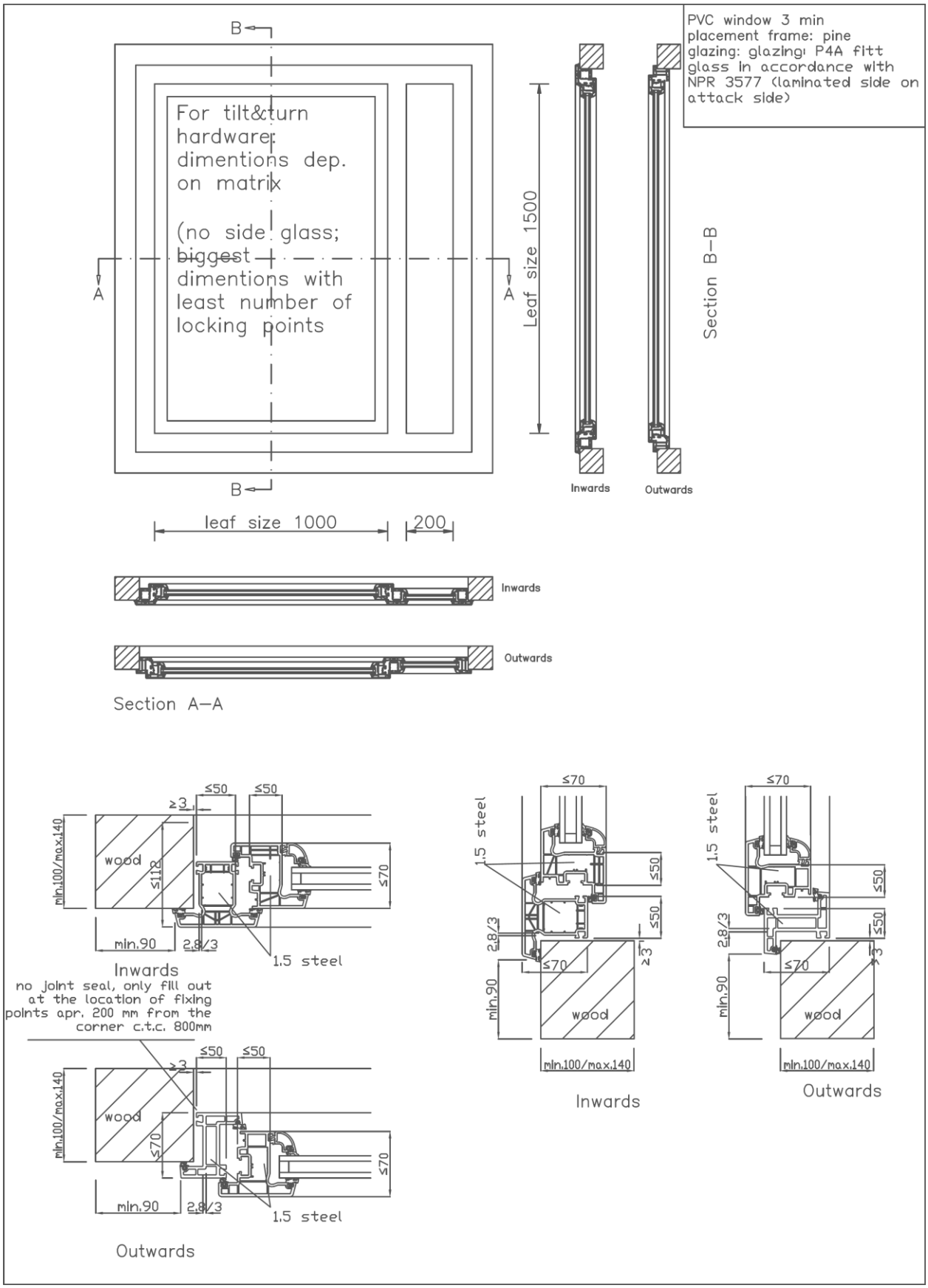
Doorsnede A-A

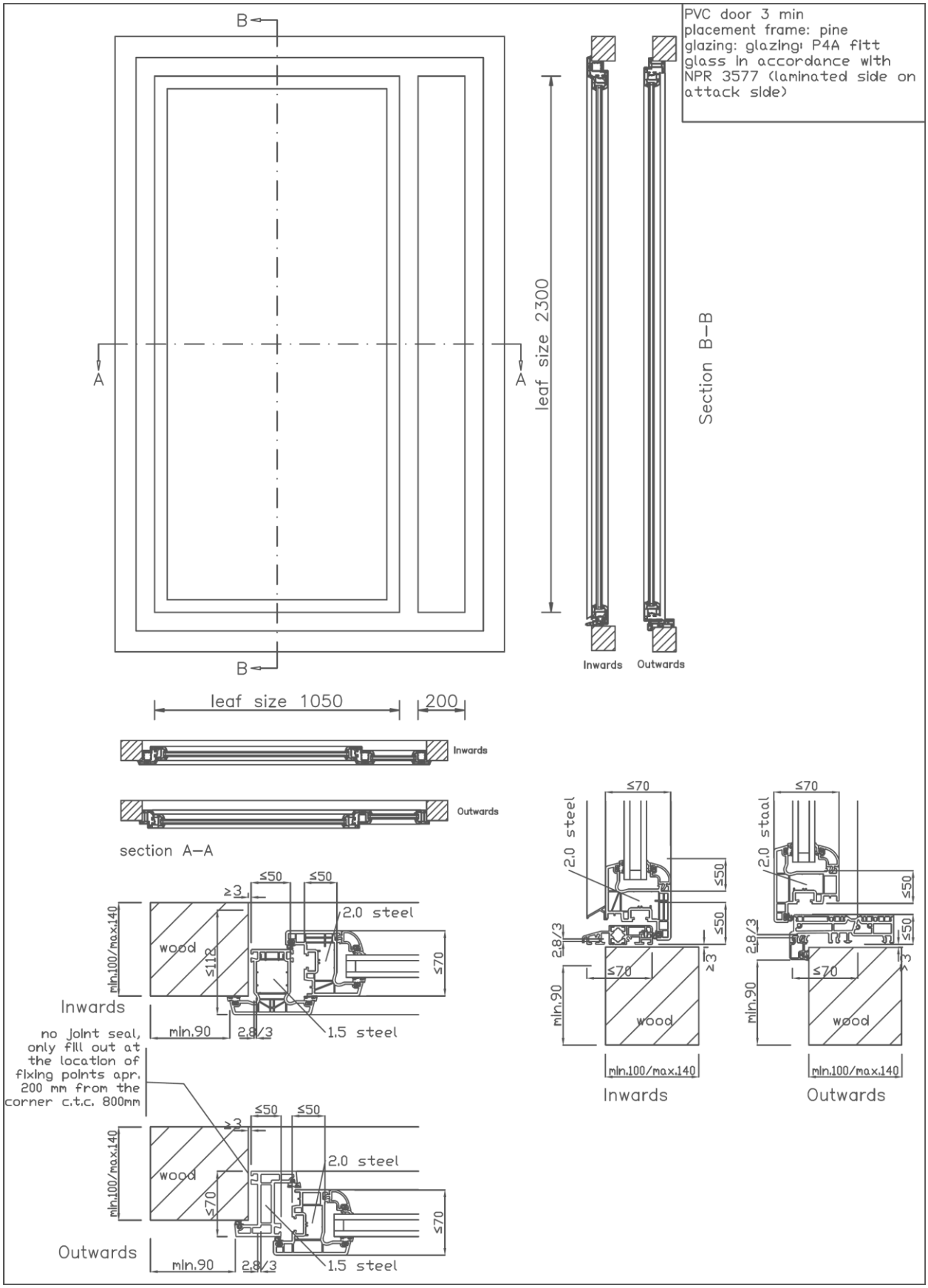


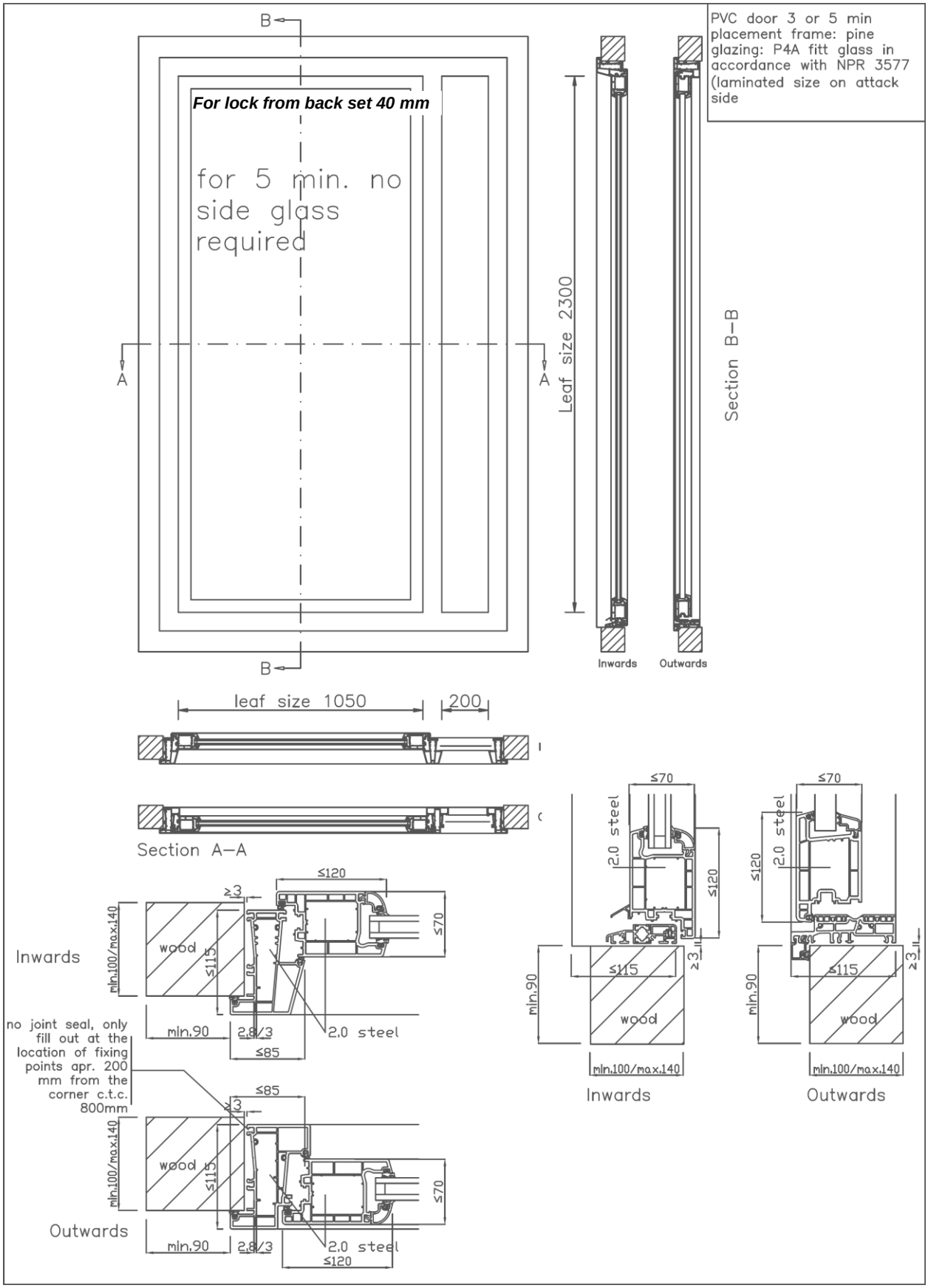


Vast Schuif

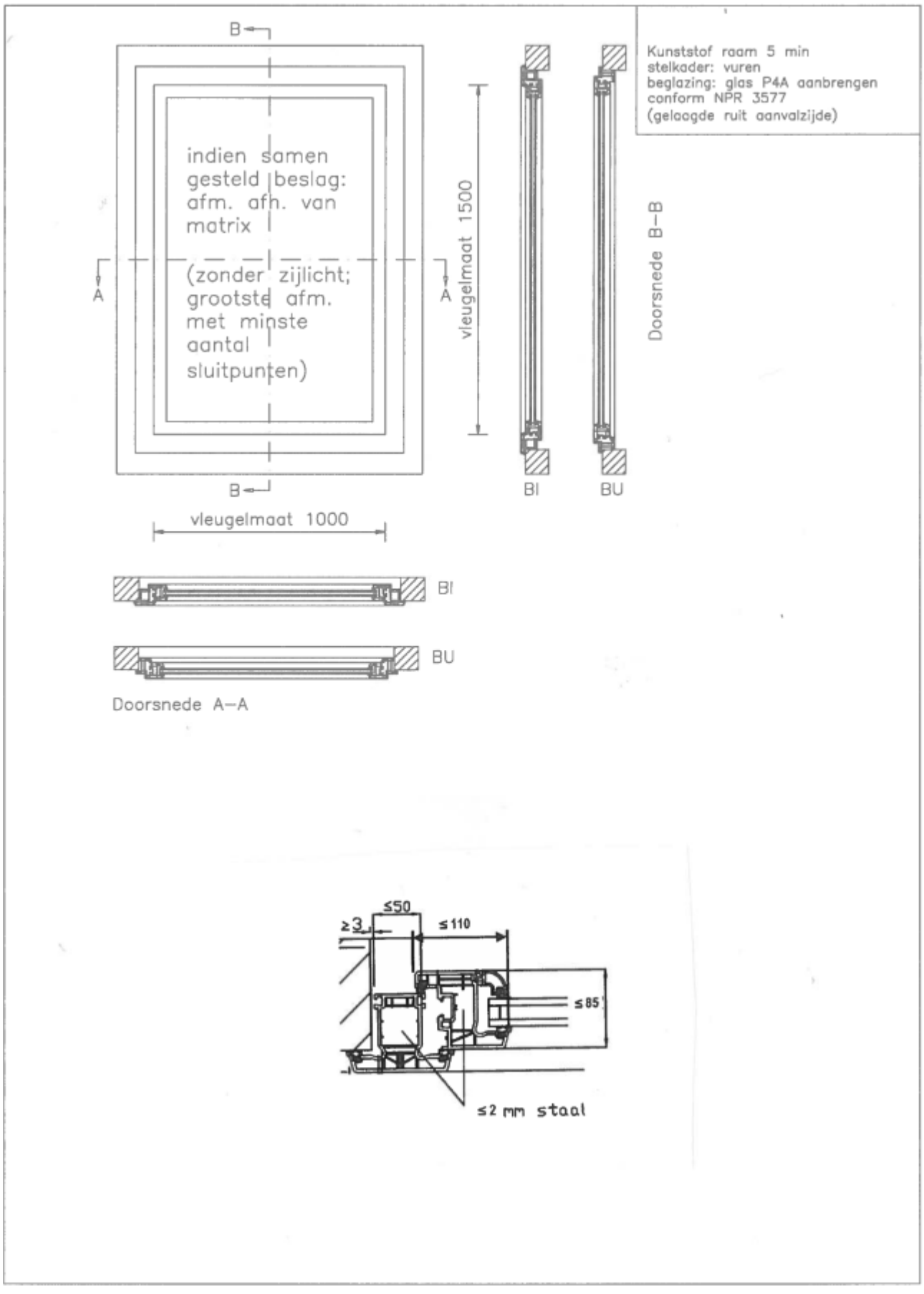
PVC 3 minutes (2-star)

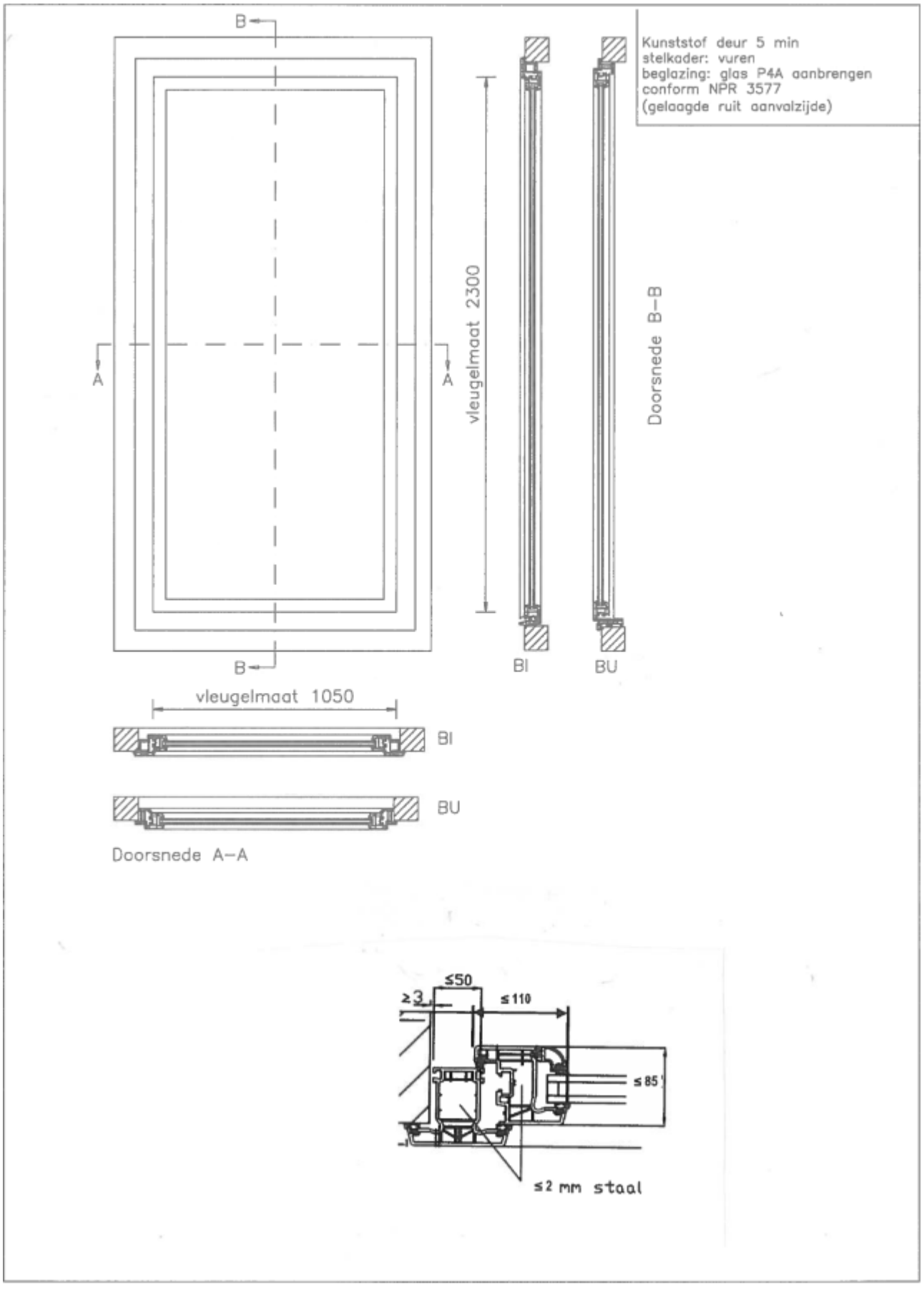



PVC door 3 min
placement frame: pine
glazing: glazing: P4A fitt
glass in accordance with
NPR 3577 (laminated side on
attack side)
B
A
A
B
leaf size 2300
Section B–B
Inwards
Outwards
leaf size 1050
200
Inwards
Outwards
section A–A
≤50
≤50
≥3
2.0 steel
wood
≤112
min.100/max.140
≤70
Inwards
min.90
2.8/3
1.5 steel
no joint seal,
only fill out at
the location of
fixing points apr.
200 mm from the
corner c.t.c. 800mm
≤50
≤50
≥3
2.0 steel
wood
≤70
min.100/max.140
≤70
Outwards
min.90
2.8/3
1.5 steel
≤70
2.0 steel
≤50
≤50
2.8/3
≥3
≤70
min.90
wood
min.100/max.140
Inwards
≤70
2.0 staal
≤50
≤50
2.8/3
≥3
≤70
min.90
wood
min.100/max.140
Outwards

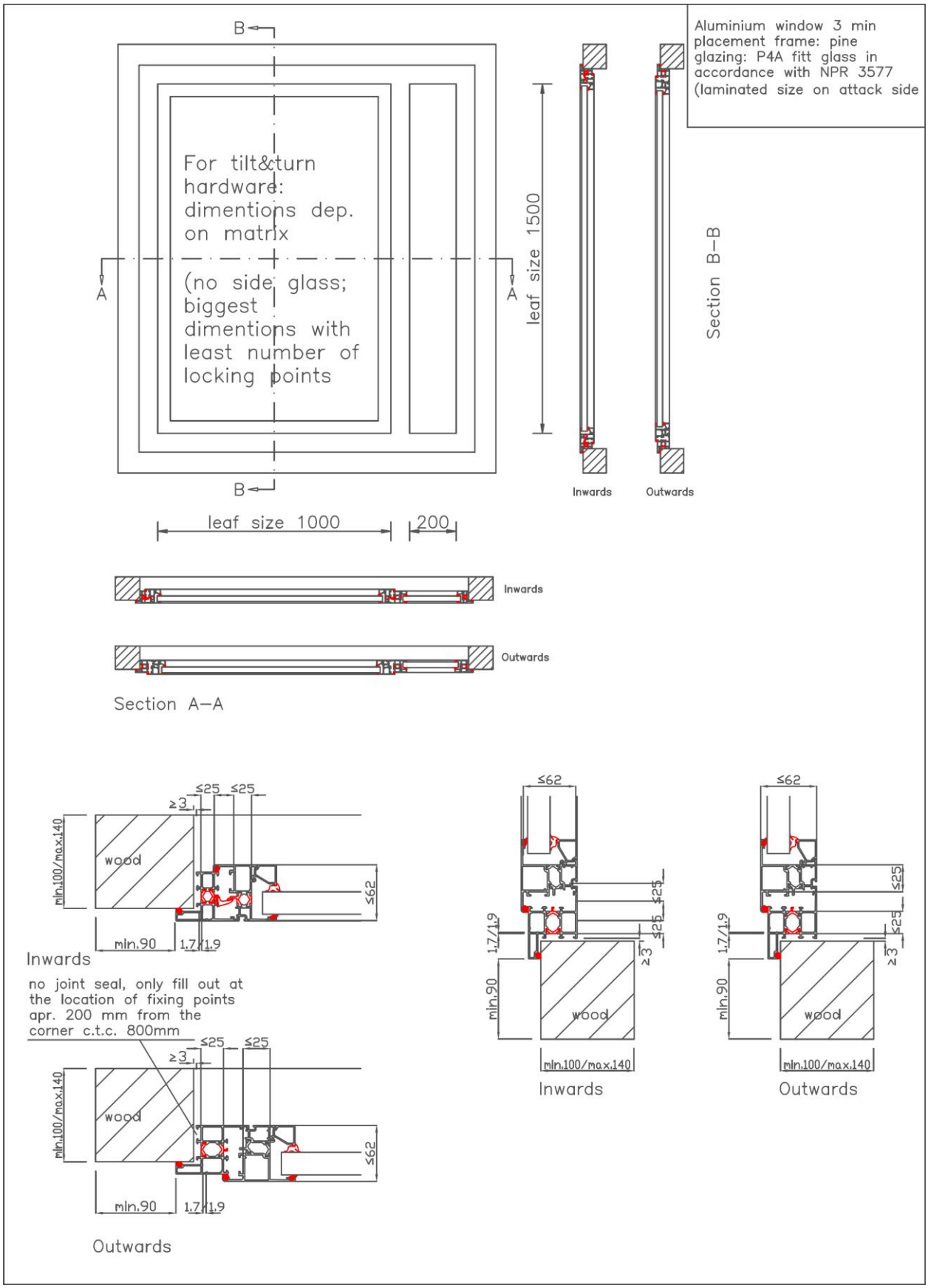

PVC door 3 or 5 min placement frame: pine glazing: P4A fitt glass in accordance with NPR 3577 (laminated size on attack side
For lock from back set 40 mm
for 5 min. no side glass required
B
A
A
B
Leaf size 2300
Inwards
Outwards
Section B–B
leaf size 1050
200
Section A–A
≤120
≥3
≤70
wood
≤115
min.100/max.140
Inwards
min.90
2.8/3
2.0 steel
≤85
no joint seal, only fill out at the location of fixing points apr. 200 mm from the corner c.t.c. 800mm
Outwards
≤70
2.0 steel
≤120
≥3
≤115
wood
min.90
min.100/max.140
Inwards
Outwards

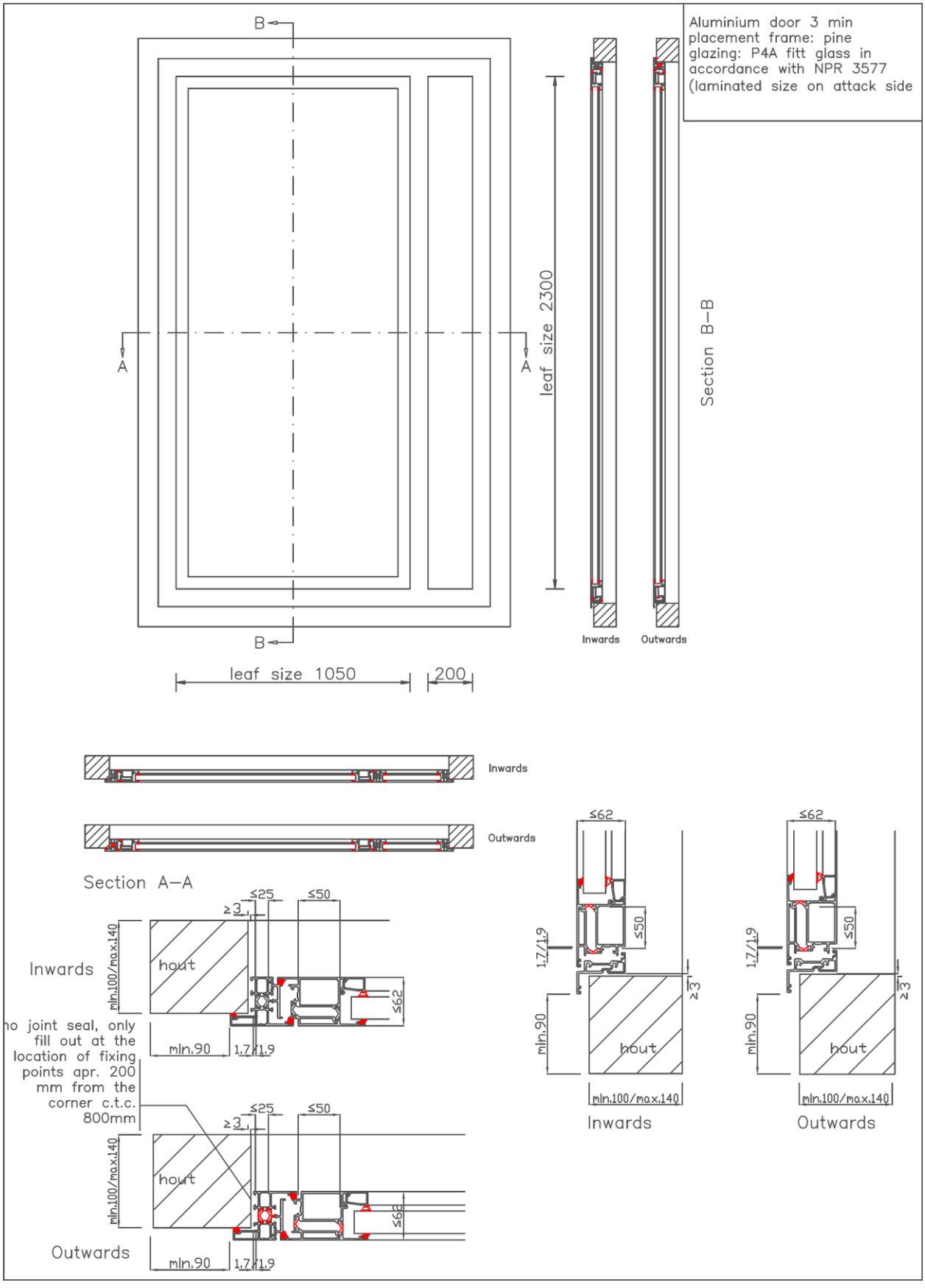
PVC 5 minutes (3-star)



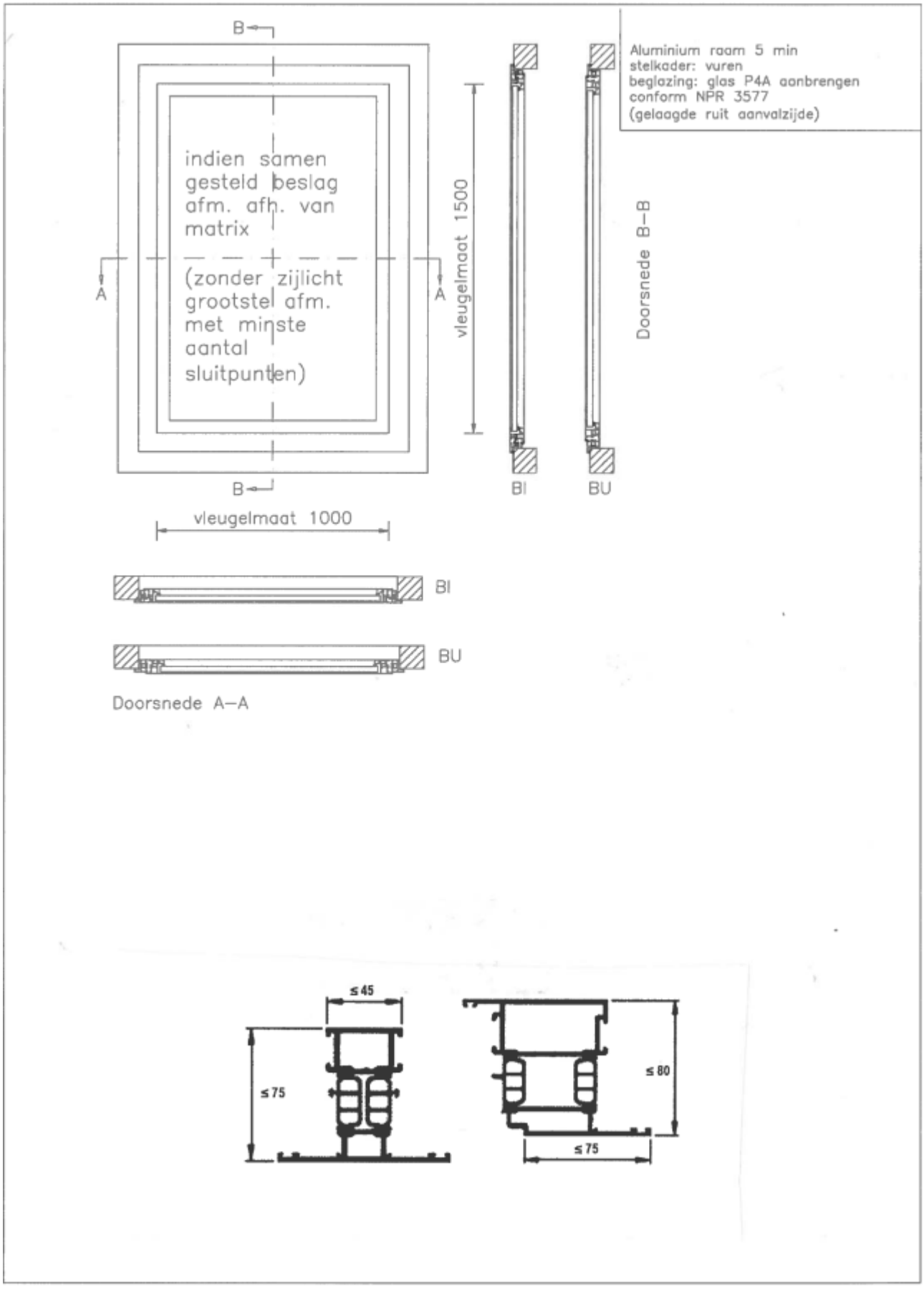

Kunststof deur 5 min
stelkader: vuren
beglazing: glas P4A aanbrengen
conform NPR 3577
(gelaagde ruit aanvalzijde)
B
A
A
B
vleugelmaat 2300
BI
BU
Doorsnede B–B
vleugelmaat 1050
BI
BU
Doorsnede A–A
≤50
≥3
≤110
≤85
≤2 mm staal

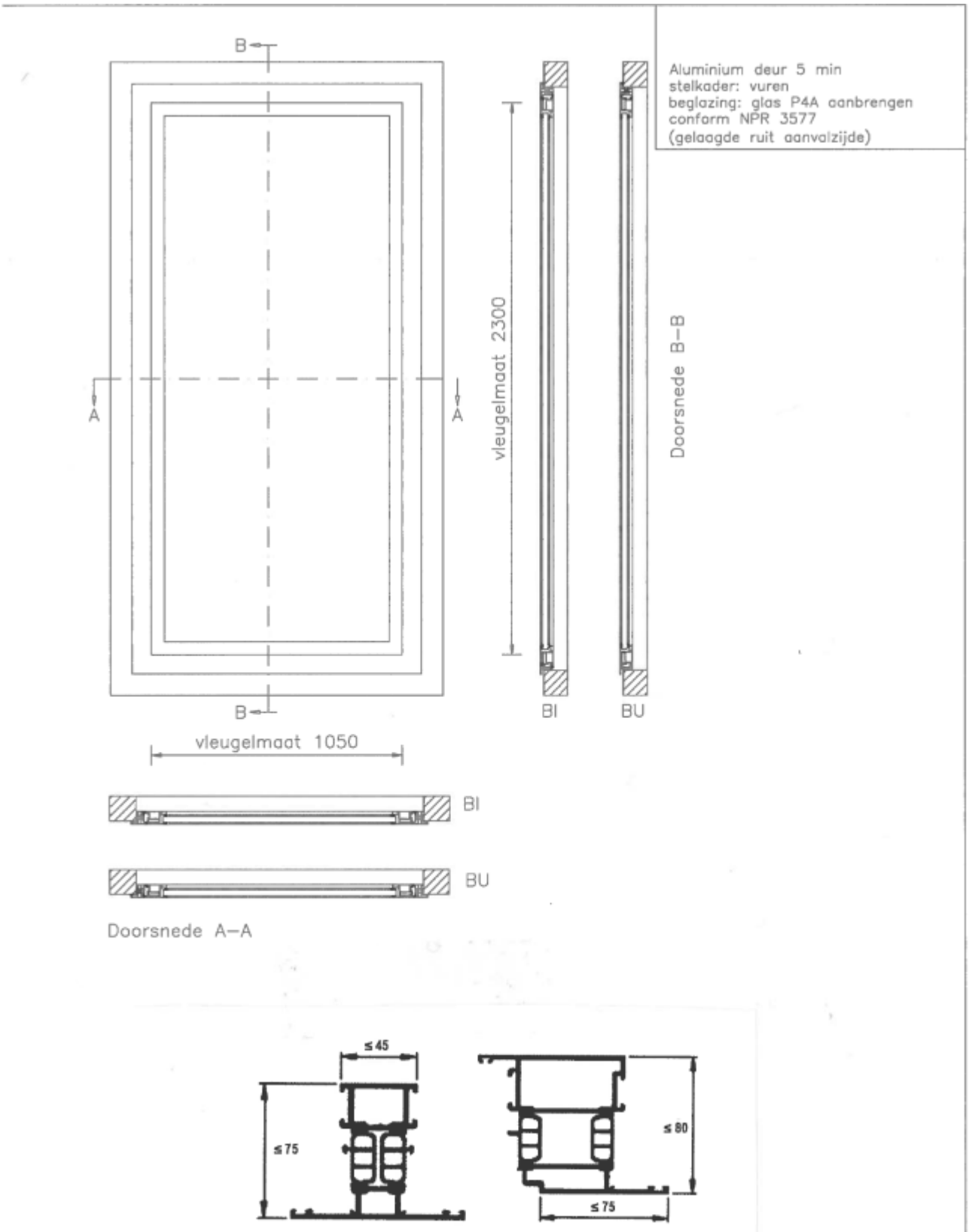
Aluminium 3 minutes (2-star)




Aluminium door 3 min
placement frame: pine
glazing: P4A fitt glass in
accordance with NPR 3577
(laminated size on attack side
B
A
A
B
leaf size 2300
leaf size 1050
200
Inwards
Outwards
Section B–B
Inwards
Outwards
Section A–A
≤25
≤50
≥3
Inwards
hout
min.100/max.140
≤62
min.90
1.7/1.9
no joint seal, only
fill out at the
location of fixing
points apr. 200
mm from the
corner c.t.c.
800mm
Outwards
≤62
1.7/1.9
≤50
≥3
min.90
hout
min.100/max.140
Inwards
Outwards

Aluminium 5 minutes (3-star)




Aluminium deur 5 min
stelkader: vuren
beglazing: glas P4A aanbrengen
conform NPR 3577
(gelaagde ruit aanvalzijde)
B
A
A
B
vleugelmaat 2300
BI
BU
Doorsnede B–B
vleugelmaat 1050
BI
BU
Doorsnede A–A
≤ 45
≤ 75
≤ 80
≤ 75